INTERNET LITERACY HANDBOOK

" Supporting users in the online world

Building a Europe
for and with children
www.coe.int/children

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

INTERNET LITERACY HANDBOOK

Supporting users in the online world

Council of Europe

Table of contents

Acknowledgments

Foreword

▬ How important is it to be Internet literate? The short answer to that is quite clear: very important. There are fast-approaching 3.5 billion Internet users, some 20% of which are in the European region. And while the Internet offers a stream of information to experience and share, navigating securely in the complex online world can be a demanding task. A basic knowledge set is required.

▬ This Handbook offers that knowledge set using language that is straightforward and easy to digest. This is not a brand new publication, but a constantly evolving set of handy tips on how to get to grips with nowadays' ever-increasing flow of information. The contents of the Handbook are equally clearly laid out online, thanks also to the winning graphics, so that the sections can be presented to groups in classrooms or community centres. In this way, it can be used as a tool for training purposes, and for all age-groups.

▬ In unravelling a myriad of complexities, the Handbook offers insights into ethical considerations and risks attached to sharing information: if we wish to use the Internet to quench our thirst for knowledge, and share our thoughts and opinions, then we must do so responsibly. Human rights tenets are just as applicable in the digital world as they are offline. They are engaged, for example, with regard to respecting others' freedom of expression and privacy online, as well as having ours respected by others. How do we ensure that our own personal data is safe? What do we do if we come across illegal content or are at the receiving end of bullying or hate speech? These topics and many, many more are presented in a way which provides practical advice and tips for an eager public, with an invitation for readers to think critically about what they see and read online, and to make informed and safe choices.

▬ If we are online to share ideas, we are at the same time building knowledge and understanding; we may challenge conventional wisdom, and we may create networks for positive change. This is particularly evident for younger generations, for whom the Internet offers endless opportunities to explore, learn, socialise and create, which in turn contribute directly to their personal development. It has become their primary source of freedom and information in growing up, and gives them the means to exercise their rights and freedoms online. Although the Internet harbours potential pitfalls, cautionary measures can be taken and sensible assistance provided. In order not to deter (especially younger) users, the Internet must not be presented as a dark place signposted with danger and caution. It is precisely in its aim of providing support in using the Internet knowledgeably, creatively, safely and fearlessly that marks the Handbook out as a unique and precious tool. If, through the Handbook, children can embrace the multitude of possibilities that the Internet has to offer, at the same time as building up their digital resilience, conscious of their own capabilities and responsibilities, then the Handbook will have served its purpose.

▬ The Council of Europe is proud to have followed the evolution of the Handbook and grateful to the many involved over the years in its initial launch, subsequent revision and edition. This tool now provides an even richer source of quality information for children, parents, teachers and policy makers of the 47 member states to be able to make the most of the Internet and to prepare future generations to use the Internet safely and confidently.

Snežana Samardžić-Marković
Director General of Democracy

Christos Giakoumopoulos
Director General of Human Rights and Rule of Law

Introduction

> Literacy is a bridge from misery to hope. It is a bulwark against poverty, and a building block of development, …a platform for democratization, and a vehicle for the promotion of cultural and national identity. … Literacy is, finally, the road to human progress and the means through which every man, woman and child can realize his or her full potential.
>
> *Kofi Annan, former Secretary General of the United Nations, January 1997-December 2006*

This is the second edition of the *Internet Literacy Handbook*, which was initially published in 2003. The first edition was revised at three-yearly intervals, in 2006 and 2009, in an effort to keep up with the challenging pace of evolution in the online technology sector. Although this edition proposes a similar structure, the content has been completely updated and new Fact sheets added, with special focus also on the technology of tomorrow.

The handbook is destined for a broad public including families, educators and policy makers; however, it also provides links to more in-depth information and resources for those who wish to delve further into the topics. At the same time, it is aimed to be instructive for young people in their teens and 20s who figure amongst the most avid users of technology and are the shapers and makers of new trends.

Above all, the *Internet Literacy Handbook* sets out to provide information and promote reflection on some of the more complex ethical, sociological and cultural issues that are intrinsically linked to digital- and media-related activities which have taken on such a large role in the lives of a majority of people in many parts of the world. The Council of Europe, which publish this handbook, has striven since 1949 to promote, protect and develop human rights, democracy and the rule of law in its 47 member states.

As technology has rapidly reached into most corners of most people's lives over the past half century, it has also impacted upon human rights, responsibilities and freedoms, and at the same time considerably extended the concept of literacy, which is at their core. The *Internet Literacy Handbook* is one of the Council of Europe's broad palette of instruments aimed at tackling the many challenges and at taking advantage of the many opportunities that have come in the wake of the Internet. Some of these instruments are referenced in the handbook.

Literacy implies the mastery of contemporary tools of communication as a means of expression and understanding – previously known in English as the 3Rs (reading, (w)riting and (a)rithmetic). But when we use digital tools and platforms to express ourselves, their very power, speed and instantaneity of dissemination turn literacy into a multilayered concept that many of us continue to grapple with. Photos, videos, limited character messages, emoticons and podcasts have become languages in their own right through tools like Instagram, Snapchat, Vine and Periscope, and interaction and real communication are only too often a faceless, electronically mediated process. This is especially the case for young people, who text, tweet, play electronic games and exchange images night and day in the online world which is woven and blurred into what adults still refer to as the "real world".

Social and cultural conventions are upturned as social media users "friend" or "unfriend" people they will probably never meet from the other side of the world. Relationships are increasingly

being created online as business partners meet and create companies through the Internet, and increasingly it is becoming the place where people first encounter their life partners. These deep changes have placed responsibility and accountability at the heart of the core set of literacy skills, necessitating a solid understanding of our own fundamental human rights and respect of the rights of others if we are to avoid the pitfalls and contribute positively to today's society.

▬▬ The *Internet Literacy Handbook* is presented as a compendium of Fact sheets in a similar format to the first edition. However, the Fact sheets have now been organised into six themed sections, enabling users to more easily download and print section by section or individually, as they wish. Each section provides an overview of its contents in the form of checklists. This is more comprehensive than a simple index would be and facilitates consultation of the Fact sheets by offering a rapid guide to the most essential points covered. Together, the sections aim to address the principal facets of the Internet, from essential information on how it works and where our data is stored, to finding quality information and connecting with people and knowledge, to getting assistance and looking ahead at where online technology may take us next. The sections constitute a tool kit aimed to help users navigate through the network of possibilities the Internet offers and, in the process, to acquire ways in which they can contribute to shaping the online world rather than being shaped by it.

▬▬ In keeping with the electronic medium in which they are presented, the Fact sheets aim to be reasonably short, easy to read and conducive to rapid searches for ideas, alerts and useful tips and links. Each begins with a state-of-the-art overview of the topic in question, before investigating a little more fully and with a little more precision just how that tool, platform or service can be used educationally to bring added value and opportunities. The users' attention is then drawn to some of the ethical aspects worthy of further reflection but, as noted above, technology is constantly on the move and hence new ethical considerations are emerging all the time. The "how to" section in most Fact sheets is a practical guide that aims to provide step-by-step information on how things actually work, or how they can be made to work so that users can get the most out of technology.

▬▬ The final sections of each Fact sheet provide ideas for classroom use, good practice examples and further information that can range to anything from links to articles and directories to further applications of that specific tool or service. These pages can be seen as a repository of the "best of the crop" that has been gathered from institutions, organisations and individuals working worldwide in social, educational, cultural and child protection fields and curated by a handful of specialists especially for handbook users. Every effort has been made to ensure that all recommendations provided are up to date, relevant and reliable for use with all age groups unless otherwise stated. Users are, however, certainly aware that in today's fast-moving world thousands of URLs (Uniform Resource Locators, otherwise known as a "link" or "weblink") are being created and deleted every day. No handbook relating to online technology could therefore guarantee that all information will remain valid and that all of the URLs it contains will continue to exist.

▬▬ The *Internet Literacy Handbook* should rather be seen as a snapshot or a "take" at a given point of time. It will need to be superimposed with new information, ideas and guidance if it is to remain fully relevant for its intended public. Readers are invited to contribute to this evolutionary process by sending their ideas, resources and good practice examples to the Children's Division of the Council of Europe, children@coe.int.

1. Internet: Anytime, Anywhere

> ,, "We are all now connected by the Internet, like neurons in a giant brain."
>
> *Stephen Hawking, theoretical physicist*

CHECKLIST FACT SHEET 1 – GETTING CONNECTED

Have you made sure that your Internet connection is secured by setting up an antivirus, a firewall and by setting a password for your Wi-Fi router?

Have you set up an acceptable use policy (sometimes called a responsible use policy) for anyone using/accessing the Internet through your network and devices?

Have you set up "guest" accounts on devices that are used by your children?

CHECKLIST FACT SHEET 2 – ONLINE PRESENCE AND THE CLOUD

Have you included contact details in your website or blog?

Have you taken steps to protect your online privacy?

Have you checked that the content that you are using for your website/blog is in accordance with copyright law?

CHECKLIST FACT SHEET 3 – WEB 2.0, WEB 3.0 AND MORE

Systematically seek permission from people featuring in the photos and videos you post online.

User recommendations on travel and product sites can be helpful, but are you sure they are real?

User-generated content fosters creativity and freedom of expression, but also places the onus on you if the Internet is to become a better place.

CHECKLIST FACT SHEET 4 – BLOGS AND VLOGS

Protect your privacy by using a pseudonym and hold back certain personal details.

Protect your blog or vlog from hackers by setting up appropriate security precautions and saving your content regularly.

Understand your blog goal and audience when posting content.

CHECKLIST FACT SHEET 5 – INTERNET ON THE GO

At what age can children safely begin to use mobile devices and which ones are most appropriate for very young children?

Do you understand geolocation and Bluetooth sufficiently to use your mobile devices comfortably and safely?

M-learning and mobile wallets are areas in which the use of mobile devices is changing the way we learn, work and shop. What do you know about these recent evolutions?

Getting connected

The Internet is a worldwide network of computers linked together through servers which function as connection nodes[1]. In June 2016 there were an estimated 3.5 billion Internet users in the world of which 614 million were in Europe[2].

How does the Internet work and why is it important to know the process? You are most likely already using the Internet on a daily basis, even more frequently than your bike or car. While you do not need to know all the technical details about how the Internet works, you should at least have a basic grasp of how it works, much like knowing how to change a tyre on your bike or check the oil level on your car.

At home, you are most likely connected to the Internet by using a router, that mysterious box that connects either to your telephone line or to your TV cable. All of your devices, be it your smart-phone or your computers are connected to that router either via an Ethernet cable or via Wi-Fi.

1. http://en.wikipedia.org/wiki/Node_%28networking%29
2. www.Internetworldstats.com/stats.htm

Now imagine that your router was connected with a cable to your neighbours' router, and your neighbour's router to the house next door etc. That is exactly what the Internet is on a smaller scale. The Internet is simply a huge number of routers connected to each other that allow you to forward and transmit information (data that contain emails, pictures, videos etc.) from one point (your home computer for instance) to another (the smartphone of your friend who is on vacation at the other end of the world).

As amazing as it may sound, there are huge underwater cables that stretch under the ocean across all continents, running directly into a cable landing point which connects into the land-based infrastructure (usually telephone lines).

So just imagine, whenever you send a picture from your computer to a friend this is what happens: your picture gets chopped up into tiny pieces of data called packets which are labelled much like an envelope in the post office (destination, origin and information on how to put that piece of data back together to recompose your picture). Instead of having information like a street name and house number, data packets contain the IP address[3] from where it was sent and the IP address of where they are supposed to go. They then go through your telephone line to your Internet service provider's facilities which are connected to the Internet backbone (which is the huge number of interconnected routers we talked about). The packets are redirected by these routers several times until they reach their destination (that's called the number of hops). But what is really the destination of your picture? If you send a picture via email for instance, the destination isn't your friend's computer, but the data centres of the email client your friend uses.

Data centres are huge warehouses filled with routers and hard drives. Your picture will be stored across multiple hard drives (to protect the data in case of hard disk failures). If your friend uses Gmail for instance, then the picture that you have sent to your friend may physically be stored on one of the Google data centres either in the United States, Ireland, Belgium, the Netherlands and many more countries[4]. And your friend, when he or she wants to look at it, sends a request from his or her computer which is redirected through the Internet backbone all the way to that data centre, which then sends on the data with your picture onto his or her computer screen.

INTERNET GOVERNANCE

But how was the Internet set up in the first place? Who is responsible for maintaining the current infrastructures and creating new ones? Who decides on standards such as IP addresses?

While the idea of hyperlinks and interconnected web pages came from Tim Berners-Lee and Robert Cailliau, working at CERN in Switzerland, the first interconnected network called ARPANET was established in the US between universities[5].

Therefore, the very first body that was responsible for the allocation of unique "addresses", which essentially allowed someone to connect to the network, was set up in the USA (IANA – Internet Assigned Numbers Authority).

As the Internet grew, so did the need to better co-ordinate the development, maintenance, stability and security of the Internet. The United States Department of Commerce pushed for a reform of IANA which became ICANN[6] (the Internet Corporation for Assigned Names and Numbers) in 1998. ICANN was officially set up as a non-profit corporation "for charitable and public purposes", with a strong "bottom-up" approach to governance, consisting in the co-ordination of thousands of stakeholders across the globe, including private sector stakeholders, civil society and governments. However, it has faced much criticism and calls for reforms from countries around the world due to its ties to the US Government and the risk of over-representing US interests.

In response, ICANN has opened up to a wide variety of stakeholders including 111 states and

---

3. https://en.wikipedia.org/wiki/IP_address
4. http://www.google.com/about/datacenters/inside/locations/index.html
5. https://en.wikipedia.org/wiki/World_Wide_Web
6. https://www.icann.org/

a number of observers, such as key telecommunications organisations and the Council of Europe. But ICANN remained criticised for its lack of democratic input and broader consultation of stakeholders, which prompted the creation of the Internet Governance Forum (IGF) in 2006 by the United Nations.

The IGF meets annually and provides the opportunity for a broad range of stakeholders, including young people, to share their views on the future of the Internet.

EDUCATIONAL BENEFITS

- The Internet offers access to a wealth of new ideas, resources, learning opportunities, information and services.

- The Internet facilitates exchange of experience and communication between users across international borders in a variety of ways: forums, e-mail, social networks, chats, video conferences and so on. It thereby offers students the opportunity to take part in projects and work with other students without the need for expensive travel.

- The Internet makes research tools accessible even to those who do not regularly visit a traditional library.

- With additional devices and software, the Internet can open up new opportunities to those with special needs.

- Learning about how the Internet is governed enables all citizens to get involved in key decisions that will shape its future.

ETHICAL CONSIDERATIONS AND RISKS

- Be aware that the Internet often provides a false sense of anonymity. Given how the Internet works, you always leave a trace whenever you go on the Internet (your IP address).

- As in the offline world, there is fraud, false information and inappropriate material for children.

- While the Internet offers a number of new possibilities, technical solutions are not always better than traditional ones. For example, e-mail has revolutionised communication and although video-conferencing can give a feeling of "almost being there", it will never replace face-to-face communication.

- Internet governance can have a tremendous impact on your Internet experience with principles such as anonymity or net neutrality in the balance. There is a constant battle between the principle of a free and open Internet and those who wish to control it. Some companies try to redirect traffic to their own websites, apps or services by providing "free" mobile Internet plans limited to those websites, apps or services, and by charging for visiting others[7]. Facebook, for instance, has created the "Internet.org" portal which is the default home page for all users who connect via their Internet service in various parts of the world, especially in developing countries[8].

- Be aware that anything you share online may be cached, stored or copied.

HOW TO

- Virtually all devices that you buy nowadays are capable of connecting to the Internet, either via Wi-Fi or mobile Internet access (smartphones and tablets, for instance, can connect via Wi-Fi or mobile Internet access), or via an Ethernet cable (most computers are equipped with an Ethernet port).

---

7. https://en.wikipedia.org/wiki/Zero-rating
8. https://en.wikipedia.org/wiki/Internet.org

- To connect to the Internet you have two main options:

  ► Contact an ISP (Internet service provider), usually a telephone or cable company, that will provide you with a username and password and sometimes a modem/router to connect to the Internet either via your telephone line or your television cable.

  ► Get a "mobile Internet" plan from your mobile phone operator. Keep in mind that the restrictions on the amount of data you can download/upload are still quite high with mobile Internet, although these will progressively diminish as more operators roll out 4G or 5G mobile telecommunications standards (with a great increase in speed).

- There are also more and more "open" Wi-Fi hotspots that you can use to connect to the Internet for free. You can find them in a variety of public places, such as a public library but also in bars, restaurants and shopping malls. Most of the time, before you connect, you will be asked to do one or more of the following: accept the terms of use, create an account using your e-mail address (be aware that your e-mail may then be used to send you advertising so be sure to create an e-mail address specifically for these situations) or enter a password to connect to the Internet. In bars, restaurants or hotels, for example, the "open" Wi-Fi is often only accessible to clients so you have to ask a member of staff to give you the password. Never share sensitive data or carry out sensitive operations such as mobile banking via public Wi-Fi hotspots.

- Most ISPs will provide you with a preconfigured router that you will just need to plug into your telephone/cable line in order to be connected. Sometimes, you will need to buy a router and configure it yourself. Be sure to check with your ISP if the router you have or that you intend to buy is compatible with your Internet subscription!

IDEAS FOR CLASSROOM WORK

On Windows 7 and above

1. Click on the "**Start**" button in Windows.

2. Type "**cmd**" in the "**search**" bar and click on the program icon that shows up in the start menu.


```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.   All rights reserved.

C:\>
```

3. Type "**tracert wikipedia.org**" and press "**enter**".

4. You will then be able to see the "**hops**" that exist between your computer and the website you are trying to reach and how much time each "hop" takes. In this example, we see that to access Wikipedia, we first go through routers of our "local" ISP (in this case Belgacom from Belgium),

then we go across the Atlantic to a router in Washington (abbreviated "was"), finally to arrive to the place where Wikipedia is hosted. Students are of course encouraged to try this with other websites. Notice how much time each step took in milliseconds.


```
C:\Windows\system32\cmd.exe

C:\>tracert wikipedia.org

Tracing route to wikipedia.org [208.80.154.224]
over a maximum of 30 hops:

  1     12 ms     45 ms      7 ms   192.168.1.1
  2     25 ms     28 ms    175 ms   1.192-134-109.adsl-dyn.isp.belgacom.be [109.134.
192.1]
  3      *         *          *      Request timed out.
  4    193 ms     39 ms     77 ms   ae-12-1000.ibrstr3.isp.belgacom.be [91.183.246.1
08]
  5     30 ms     43 ms     52 ms   ae2.bru21.ip4.gtt.net [141.136.102.217]
  6    126 ms    162 ms    133 ms   xe-7-3-0.was10.ip4.gtt.net [141.136.111.10]
  7    412 ms    388 ms    277 ms   xe-5-3-1.cr2-eqiad.wikimedia.org [173.241.131.21
8]
  8    201 ms    277 ms    185 ms   text-lb.eqiad.wikimedia.org [208.80.154.224]

Trace complete.

C:\>
```

On Mac OS X and above

1. Launch the network utility in Mac OS X (you can do this by going into Spotlight and typing "**network utility**" and clicking on the top hit).

2. Click on "**Traceroute**".

3. Enter the domain name for which you want to perform a traceroute, such as "**Wikipedia.org**" and click on "**Trace**".

4. You will then be able to see the "**hops**" that exist between your computer and the website you are trying to reach and how much time each "**hop**" takes.

Optional material for teachers

• For more information, watch the Naked Science Scrapbook's video "How does the Internet work?"[9].

• Start a classroom discussion on how online technology can benefit people with special needs, and take a look at the Council of Europe action plan to trigger ideas[10].

GOOD PRACTICE

• Choose a connection appropriate for your Internet usage. If you are regularly using services that require a very fast Internet, such as high definition video streaming, be sure to get a faster Internet connection (at least 20 megabits per second, which is equivalent to ADSL2+). More especially, look for an Internet connection with no limitations to the amount of data downloaded. If you only require the Internet to read the news and send e-mails, then virtually any basic Internet subscription will be sufficient for you[11].

• Always turn off your devices (computers) or disable the Wi-Fi connection on your smart-phone/tablet when you go to bed. Leaving your devices connected may increase the security risk to your data and might also pose health risks (see Fact sheet 19 on security).

---

9. https://www.youtube.com/watch?v=oj7A2YDgIWE
10. https://www.coe.int/t/dg4/majorhazards/activites/2013/DIDRR/Action_Plan_CoE_Easy_to_Read_13nov08_EN.pdf
11. www.cnet.com/internet-speed-test

- Be sure to know how to access the configuration page of your router. Most often, if you type one of the following IP addresses into your browser you can access it: 192.168.1.0 or 192.168.1.1. Why is this important? Most Wi-Fi configuration pages have "default" administrator accounts with very basic usernames and passwords (for instance username "admin" and password "admin"). It is very important to secure the access to your router's configuration page as it can easily be used to change your settings or gain access to your home computer network.

- Sit next to your children whenever you can while they are surfing the Internet, in order to stimulate discussion about their online experiences and to increase trust; make it a challenge to learn together.

- Take an active interest in Internet governance and make your voice heard in public debates over fundamental principles such as anonymity, security or net neutrality.

- Draw up an acceptable use policy (AUP)[12] or responsible use policy (RUP) if others will be using the computer or network you are responsible for.

FURTHER INFORMATION

- The List is a worldwide directory of ISPs. *<http://www.thelist.com>*.

- Education websites such as European Schoolnet at *<http://www.eun.org>*, Global SchoolNet at *<http://www.globalschoolnet.org/GSH/>* and Education World at *<http://www.educationworld.com/>* offer resources and collaborative projects.

- Advice on writing an AUP can be found via Education World, an online portal for teachers and education professionals: *<http://www.educationworld.com/a_curr/curr093.shtml>*.

- The Insafe portal offers resources and advice on how to get connected and surf safely: *<https://www.betterinternetforkids.eu/>*.

- The official website of the Internet Governance Forum enables discussion to take place on public policy issues linked to the Internet: *<http://www.intgovforum.org/cms/>*.

- The following Wikipedia page contains various information about net neutrality: *<https://en.wikipedia.org/wiki/Net_neutrality>*.

- Information on ICANN can be found on their official website: *<https://www.icann.org/>*.

---

12. http://en.wikipedia.org/wiki/Acceptable_use_policy

Online presence and the cloud

Do you have something that you want to share with the world and you need a place to share it online?

▬▬ While websites were one of the first ways to share online, more and more alternatives to websites have emerged over the last decade or so. At the beginning of the Internet, setting up a website was no joke: it was rather costly and demanded some coding skills. Nowadays, however, you do not even need to be an IT specialist to set up and design your own website. But before you do, always take the time to consider all your options.

▬▬ In summary, you must understand what you want to share and how you want to share it.

▬▬ Do you want to share very specific content (images, video, texts, etc.) or do you want to share a wide range of content? Do you want to have full control over the entire process of creativity or do you prefer to work from a preset template that you can modify to some extent? What would be the purpose of sharing content and why do you need it? Who is the audience – the world, district, hometown or just students and parents? How much are you willing to pay for sharing content online?

The diagram below illustrates a non-exhaustive list of ways you can share content, organised along a continuum that goes from total control/customisation to less control/customisation.

| Web-hosting without a template | Web-hosting with a website builder | Blogs | Discussion forums | Specific content sharing: Soundcloud, YouTube, Instagram, Flickr, etc. |

More control ← → **Less control**
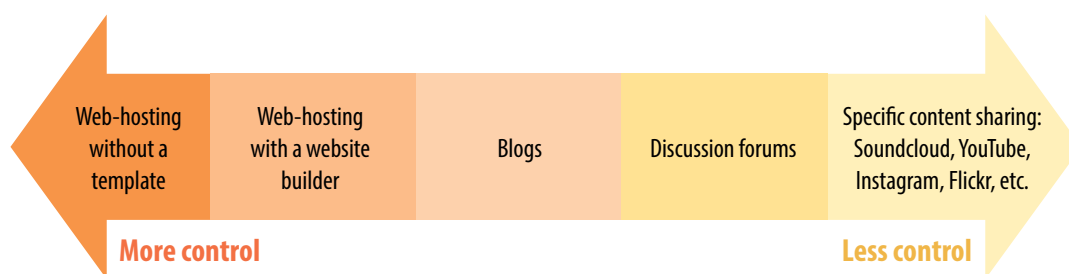
If you want to be completely free with regards to both content and design, then you should opt for web-hosting without a template. But remember this comes at a cost and you will have to purchase, in most cases, a domain name (for instance, *<www.mywebsite.com>*). If you do not wish to learn how to code but still want to share a wide variety of content and have high flexibility of design, you can go for web-hosting with a website builder or for a blog (which will sometimes have even less flexibility of design). Discussion forums are already pretty specific: you can set up discussion forums or message boards for your school, for instance. And finally, if you just want to share pictures, videos or music, you can choose to set up an account on a service that is specialised in hosting that type of content. In the end, your content, whatever it may be, will end up somewhere on the server of the hosting service you will choose: it will be in the "cloud".

Also keep in mind that while many of these services exist for free, this often means that your viewers might be exposed to more or less intrusive advertising (that is, advertising that greatly hinders the user experience, such as numerous pop-ups, website overlays, an excessive number of banners, etc.).

EDUCATIONAL VALUE, WHY IS IT RELEVANT, IMPORTANT?

Developing an online presence and sharing content online has great educational value and helps develop a number of skills.

- **Content management/organisation:** whether you decide to build a website or set up a photo gallery, your content has to be organised in a simple way for users to find what they are looking for.

- **Design:** your online identity will often be linked to a logo, an image, your choice of colours, the layout of your website, all of which are part of design work.

- **Digital skills:** quite obviously, developing an online presence will boost certain digital skills such as coding (for example HTML, PHP, HTML5, Javascript) if you opt for building a website. But even with other options, you will have to learn about search engines and your content visibility, file formats, etc.

- **Communication/writing skills:** unless you plan to share content without comments, you will have to brush up on your communication/writing skills in order to catch your users' attention and interest.

- **Marketing skills:** with so many people online, it is easy to go unnoticed. Building your reputation and increasing your online visibility is linked to knowing how to sell yourself and promote what you have created or shared.

- **Teamwork:** additionally, should your online presence be a shared project among your friends/classmates/students, then it will also boost your teamwork skills. Managing a website is no easy task and the job often needs to be organised and split between several people: the administrator, designer, content writer, etc.

- **Secondary benefits:** by creating a website on a specific topic, for example a website about mathematics for a school project, you inevitably also deepen your understanding and knowledge about that topic.

ETHICAL CONSIDERATIONS AND RISKS

Should you wish to share personal content or create a personal website, you will be solely responsible for what you post. You (and your parents if you are a minor) could find yourself in difficulty for a number of reasons.

Legal reasons

The limits of "freedom of expression": this right is not absolute and there are some limits to its exercise. The limits to freedom of expression have to be stated by law in a clear way, they have to be necessary in a democratic society (proportionate) and have legitimate objectives (Article 10.2 of the European Convention on Human Rights states that "[i]n the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary"). These limits may vary from one state to another but there are some "broad" considerations that you should bear in mind:

▶ defamation[1];

▶ hate speech[2];

▶ sharing someone else's personal data[3];

▶ storage of data – if you opt to use cloud services, find out beforehand where your data will be stored; it is your right and responsibility to maintain control over its use and accessibility [4];

▶ encouragement of terrorism:

- <https://goo.gl/cv9XDR>;

- <https://goo.gl/Tq3UDp>;

▶ intellectual property: are you sharing content that is not your own? Then be sure to check whether you are allowed to share it or not. Commercial content is protected under copyright law and you need specific authorisation from the copyright holder to use it. Certain artists or creators publish content under a specific "licence", often called "Creative Commons". Depending on that licence, you may be able to use the content without having to credit the author, as well as use it for commercial purposes. As regards copyrighted material, if you want to use it, you need proper authorisation from the organisation/individual owning the rights (record company, film studio, etc.).

Any of the actions above could get you into some form of legal trouble.

Personal reasons

• Over-sharing: bear in mind that whatever you share will most likely be accessible to anyone across the entire world. Sharing your private summer vacation photos, for instance, with location information (GPS) embedded in them, could enable strangers to track you, or thieves to know exactly when you are "out of town" so they can swoop down on your home. Be strategic in what you choose to share.

• Online reputation: while you may have the illusion that you can remain anonymous online, there are many ways for people to find out your true identity. Law enforcement authorities have the necessary means to track down Internet users under certain conditions (in most cases, a court warrant). Whenever you share something online, be aware that it will contribute to your online and offline reputation.

---

1. https://en.wikipedia.org/wiki/Defamation
2. https://en.wikipedia.org/wiki/Hate_speech.
3. http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
4. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

- If you share offensive or silly content online, it may affect your current and future social and professional life. For instance, if you want to vent your frustration, talk to trusted friends/family, yell into your pillow, but do not send out a tweet to the whole world as it may come back and haunt you forever. Take a look at the Web We Want website[5] to learn more about protecting your online reputation.

Should you wish to share other forms of content (for example, something from your school), or create an official website on behalf of your school, there are a few other points to bear in mind:

- School policy on Internet safety and acceptable use must be clearly defined before creating an official website or having students participate in website-building competitions.

- The layout and the way photos are used should reflect school Internet safety policy.

- Because of safety and privacy concerns, many schools do not provide the names, or only give first names, of those in photos they publish. This is something to consider when you set up your website: what is your safety protocol in this matter?

- It is a good idea to screen all external hyperlinks to other websites in order to ensure integrity of information and that the website(s) adequately reflect(s) the school's stance on Internet safety.

- If you are a teacher, your school will need to decide whether your Internet access will be filtered (unless it is legally required) or teach your students to be more "streetwise". Many schools find a combination of both techniques to be effective. Also, when students create a website as an assignment, remember that it can be visited by users from all over the world. Think of these websites as a kind of public relations tool for your school. Therefore it would be wise for you as a teacher to supervise students' work and guide them during the creative process.

- Teachers, and in some cases parents, are ultimately responsible for all work students produce. Therefore, teachers need to have the power to refuse web pages or remove them from a school or project website. In order to adequately supervise students' work, teachers should always have access to passwords[6], websites[7] and so forth.

HOW TO

- Unless you want to pay for a professional web-hosting service and have your own domain name, getting started with sharing content online is not too complicated.

- Most services you will use, be it web-builders, blogs or vlogs (see Fact sheet 4) have built in tutorials to help you get started.

- Setting up a website from scratch, however, will require you to acquire a certain number of skills. Fortunately, nowadays, there are literally millions of ways to learn how to code in order to create a website. Some of the most popular include Codeacademy[8] and W3schools[9]. But never stop at that. Always take the time to do some research online to find other material, in your language or suited to your needs.

- Also, applying for professional web-hosting requires you to provide additional information besides your e-mail address, such as your real name, address, phone number and especially some payment information such as a credit card. Therefore, children and young people should always be sure to seek guidance and support from an adult (teacher, parent) beforehand.

---

5. http://www.webwewant.eu
6. http://en.wikipedia.org/wiki/Password
7. http://en.wikipedia.org/wiki/Website
8. www.codeacademy.com
9. www.w3schools.com/

IDEAS FOR CLASSROOM WORK

Building the online presence of your school

When used correctly, a school website, blog, vlog or similar can serve as a powerful tool to draw together the many different facets of a community. It can foster a sense of cohesion and is a valuable communication tool, making information easily accessible to all parties. Here are some helpful suggestions for web content.

- Teachers could provide lesson plans or overviews of what students did during a certain period.
- Administrators might post schedules or announcements.
- Children and young people may want to publish art, poems, stories, reports or other work.
- Parents can use the site to announce parent-teacher activities, such as festivals or other gatherings.
- The community at large may use it as a forum for announcements about soccer teams, field trips, the police, road work and so forth.

A wide variety of content may enrich a website, blog or vlog but a wide base of contributors can also make Web maintenance chaotic. It is important that a small team of people is chosen to be responsible for collecting and editing content. This task might be best carried out by a teacher or administrator, or another person chosen to function as the information and communication technology (ICT) co-ordinator.

GOOD PRACTICE

- Keep track of all your accounts. Create folders in the e-mail address you use to subscribe to these services and sort your e-mails to always find important information about your accounts such as your username.
- Always use your e-mail address, not your social networking account, when registering to important online services like website accounts, blogs, vlogs or similar. As convenient as it may seem to register to services using Facebook, Google+ or other social network accounts, do not forget that you thereby agree for these services to access large parts of your information. Also, while some social networks seem like they will go on forever, should their services terminate one day you may not be able to log into your account (for instance, when there is insufficient take up of a tool by the public, that tool may become obsolete).
- Sharing content online via a website, blog or vlog is a great opportunity to share your views but you may wish to protect your privacy by using a pseudonym and holding back certain personal details.
- Start small, take your time to learn and experiment before going live with your content or introducing it into the classroom. It might help to visit other websites, blogs or vlogs for ideas and inspiration.
- Always include key contact information such as the school address and the school phone number inside your school's website, blog or vlog.
- Make sure your web content is user- and device-friendly. Nowadays, more and more people access web content via their mobile phones, and this often requires a separate layout and design. Making your web content accessible to users with disabilities is also good practice. Have a look at some of the resources on this website: *<http://www.w3.org/WAI/gettingstarted/Overview.html>*.
- Whenever possible, make your web content multilingual so that non-English speakers can also benefit from your content.

- This article on digital trends gives more information about website builders: *<http://web.archive.org/web/20160622040107/http://www.digitaltrends.com/computing/best-website-build-websites-free/>*.

- A Wikipedia entry tells you more about online reputation management: *<https://en.wikipedia.org/wiki/Online_presence_management>*.

- The data protection Fact sheets from the EU Commission on the new General Data Protection Regulation (GDPR) include the "right to be forgotten": *<http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf>*.

- Relevant UN Convention on the Rights of the Child articles:

  Article 13 – Children have the right to get and to share information as long as the information is not damaging to them or to others.

  Article 16 – Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

  Article 29 – Education should develop each child's personality and talents to the full. It should encourage children to respect their parents, and their own and other cultures.

  Article 31 – All children have a right to relax and play, and to join in a wide range of activities.

Web 2.0, Web 3.0 and more

Web 2.0 enables us not only to download and consume but also to upload and create. The term Web 2.0 refers to a perceived "second-generation" of web-based services that emphasise user-generated content, usability and interoperability. Typical examples are social networking sites (see Fact sheet 8), wikis, communication tools and folksonomies, which all facilitate online collaboration and sharing among users. Rather than referring to any specific technical updates, Web 2.0 encompasses cumulative changes, building on the interactive facilities of "Web 1.0" to provide "network as platform" computing, which allows users to run software applications entirely through a browser.

▬▬ Users can own the data on a Web 2.0 site and exercise control over that data, through an "architecture of participation" that encourages users to add value to the application as they use it. This offers huge advantages over traditional websites, which limit visitors to viewing and whose content only the site's owner can modify. Web 2.0 sites often feature a user-friendly interface based on merged or "rich" media, that is advanced technology such as streaming video, downloaded applets (programs) that interact instantly with the user, and content that changes when the cursor is placed over it.

WEB 3.0 AND MORE

▬ Web 3.0 (sometimes you may also see Web 4.0, 5.0, etc.) is a more widely debated term. Described by some to be the evolution and extension of Web 2.0, other specialists define it as a sort of "connective intelligence" that connects data, concepts, applications and people and, according to many, will ultimately start generating data on its own. Some people prefer the term "Semantic Web" whilst other experts define the Semantic Web as just one of several converging technologies and trends that will define the next big Web evolution.

▬ Other types of networks also exist. The darknet (or dark net) is a network that exists as an overlay to what we call the World Wide Web, and can only be accessed with specific software, configurations or authorisation, usually using special communications protocols and ports. Friend-to-friend (F2F – only direct connections between people who know each other) and peer-to-peer networks (between people with equal user privileges) are usually used for file sharing. Networks such as Tor work via an anonymised series of connections and can therefore be more easily used for illegal activities.

IMPLICATIONS FOR SCHOOLS

▬ Web 2.0 tools facilitate creativity, collaboration and communication, and can have a profound effect on learning. They have promoted new pedagogical models such as flipped classrooms where students do many traditional classroom activities at home[1]. Because many Web 2.0 tools are free programs, they have helped reduce the cost of software and encouraged the development of new licencing models for schools.
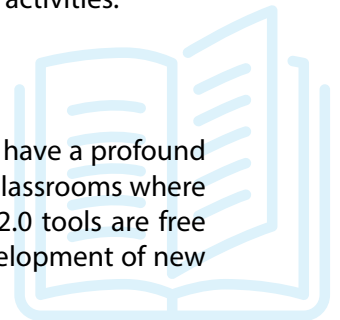
There are many distinctions between Web 1.0, 2.0 and 3.0 as illustrated in the table below.

Web 1.0	Web 2.0	Web 3.0
Application based	Web based	Multi device/dynamic applications
Isolated	Collaborative	Distributes customised content
Licenced or purchased	Free	Converged multi-licence media
Single creator	Collaborative creation	Creators and devices interact
Proprietary code	Open source	Collaboratively-built, executable
Copyrighted content	Shared content	User- and machine-generated content

▬ Four of the most commonly used Web 2.0 technologies are social networks (see Fact sheet 8), messaging, creating and watching videos and films (via podcast, MP4s, etc.), and wikis, though a number of other technologies exist.

▬ **Podcasting**[2] was born with the launch of the iPod (the Apple portable media player launched in 2001) and is a derivative of the words "iPod" and "broadcast". It was a way to share audio files over the Internet for playback on mobile devices or computers, and was also known as MP3 (MPEG digital file with an audio layer). Today most mobile devices have video-recording facilities and the MP3 has been overtaken by the MP4, a multimedia format that stores both audio and video. Podcasts and MP4 videos make it easier for teachers and pupils to bring the outside world into the classroom and share events and experiences.

▬ **Video-sharing** has become hugely popular since the launch of YouTube in 2005, and is nowadays also possible through many social media platforms. Teachertube[3] is a site dedicated to teachers

---

1. https://en.wikipedia.org/wiki/Flipped_classroom
2. http://computer.howstuffworks.com/internet/basics/podcasting.htm
3. www.teachertube.com

for educational use, based on YouTube[4], which can also be used by schools and organisations to set up their own video-sharing channels. Video sharing sites[5] are usually searchable and allow users to post, comment on, tag and watch videos. Many communities exist for producing and sharing videos around a common interest. More recently, sites have appeared which allow users to edit their video clips online and add sound, subtitles and so on. An example is Jumpcut[6].

Wikis are web pages that allow readers to interact and collaborate with others, as such pages can be edited or added to by anyone. A wiki is a superb Web 2.0 tool for collaborative written work in schools. For example, Google docs[7] enables users to work collaboratively on texts, slide presentations and tables. Another well-known example of a wiki is Wikipedia, a collaborative encyclopaedia which now includes more up-to-date entries than the Encyclopaedia Britannica.

Social bookmarking allows users to share their user-generated Internet favourites or bookmarks. Traditionally, users would have a list of favourite websites as part of their own Internet browser. Now, social bookmarking allows these lists to be shared easily so that anyone can use them. The content can be classified using tags to make them easier to search and use. The Delicious[8] website and app is an example of social bookmarking and shows users how many other people have saved a particular site.

Photo sharing is a popular tool that allows users to share photographs with family and friends. One example is Flickr[9], which allows users to post photos and then invite others to view them either individually or as a slide show. Notes and tags can be added to each photo and others can leave comments too.

Photo editing and enhancing software is now available online and allows users to improve their photos. Examples of this increasingly popular application are:

- Picasa (Google) <*http://picasa.google.com*>
- iPhoto (Apple) <*www.apple.com/iphoto*>
- Photo Story (Microsoft) <*http://microsoft-photo-story.en.softonic.com*>.

ETHICAL CONSIDERATIONS AND RISKS

- Web tools enable anyone to upload or edit material on the Internet, and content may not always be correct or factually accurate. This underlines the importance of providing young learners with broad opportunities to develop the media skills necessary to evaluate sites and content for validity and bias.

- Educators should not take the simplistic line that any fake content is necessarily bad – it may be an extension of play-acting online and may also have educational value (e.g. fake profiles of famous figures from history on social networking sites).

- Web tools and apps offer boundless opportunity for users to publish information about themselves and others. They must nevertheless remain vigilant to the risks of self-disclosure and loss of privacy. The rule of thumb is not to publish anything not meant for the whole world to know about (see Fact sheet 8 on social networking).

- It takes time and effort to integrate technology in the learning process, so before embarking on this process make sure that the use of Web 2.0 and Web 3.0 tools will have meaningful consequences for your learners.

- All Web 2.0 tools are not born equal and do not have the same philosophy or business model. Beware that while a website like Wikipedia has a non-commercial, independent, volunteer-based, collaborative approach, many social networks, such as Facebook, have a commercial purpose.

---

4. https://support.google.com/youtube/search?q=teachers+channel
5. http://computer.howstuffworks.com/internet/basics/video-sharing.htm
6. www.jumpcut.com
7. https://www.google.com/docs/about/
8. https://del.icio.us
9. www.flickr.com/

- The content that you feed into Wikipedia will be used for the benefit of the community whereas the content that you feed into Facebook will be used, among other things, to show you personalised advertising.

- Rating products and services has become popular through Web 2.0/3.0 capabilities. However, critical judgment is more than ever necessary because, even on the most popular sites of this type, ratings are not necessarily reliable – paid recommendations are increasingly common.

IDEAS FOR CLASSROOM WORK

- **Internet usage:** the most popular online activity for 86% of Internet users is socialising, followed by getting information (around 50%) and career- and commerce-related activities (approximately 25%)[10]. Discuss Internet usage statistics with your pupils/children. How does their Internet usage compare with other young people in their country and other countries across the world, and with usage a decade ago? What are some of the impacts this could have?

- **Video:** students can make their own videos to share their views and opinions about a given topic more widely. Get your students to work in teams, prepare a storyboard and use their mobile phone to create the video. This will provide an opportunity to discuss topics such as copyright (see Fact sheet 14), getting the filmed/photographed person's consent (or their parent's permission in the case of minors) before uploading images to Internet, and so forth. They can share their video through your class or school website, or use a dedicated channel on YouTube[11] to reach millions of Internet users. Some schools are now using video to record lessons to enable those students who were absent to catch up on the lessons they have missed.

- **Wikis:** check out the wikis that are best adapted to your own educational setting (see further information), then set a collaborative piece of work for your students. You will be able to actively monitor the work of individual students and keep a record of all the changes that are made. Wikis provide ideal opportunities for students to work across schools and countries in true collaborative projects.

- **Social bookmarking:** set a specific research project and divide up the tasks to individual learners or groups. You can use a search engine to find a social bookmarking tool that suits your needs. Each group can use social bookmarks to compile a detailed set of relevant links. One advantage is that learners do not have to rely on accessing the same computer each time they want to continue with a piece of work as their favourites are available from any computer at any time.

FURTHER INFORMATION

- These two wikis could be used in educational settings: *<http://mediawiki.com>* and *<http://www.pbworks.com>*.

- Teachers in several hundred thousand schools in Europe today work collaboratively within a safe learning environment with classes in other countries through the European Commission's eTwinning network at *<www.etwinning.net/en/pub/index.htm>*.

- Safety information on the use of Web 2.0 tools at home and in school can be found at *<www.betterinternetforkids.eu/>*.

- Although YouTube Kids offers fewer functions than YouTube.com for watching and sharing videos, it functions within a safe environment adapted especially for younger children and offering guidelines for parent, teachers and carers: *<https://kids.youtube.com/>*.

---

10. http://www.pewglobal.org/2015/03/19/2-online-activities-in-emerging-and-developing-nations/.
11. www.youtube.com

- Information on Web 2.0 tools for use in classroom and free downloads can be found at *<http://web.archive.org/web/20160413121845/http://www.solutionwatch.com/512/back-to-school-with-the-class-of-web-20-part-1/>*.

- Useful Web 2.0 applications for elementary schools can be found at *<http://web.archive.org/web/20150914224206/http://langwitches.org/blog/2007/12/22/best-web-20-applications-for-elementary-school/>*.

Blogs and vlogs

The online diary evolved into the modern day blog in the early 1990s. The word "blog"[1] is short for "weblog" and refers to an online journal created and published by groups and individuals. The term "weblog" was added to the Oxford dictionary in 2003. Although some politicians and celebrities have taken up blogging, blogs continue to be most closely associated with more ordinary people airing their views and talking about their daily lives.

Blogs and vlogs (video blogs) have also become platforms for social change where bloggers and vloggers highlight challenges in their lives, thereby educating readers on issues such as parenting or living with autism, or raising political awareness on various issues.

Because of the popularity of blogs, many websites have been created which offer software to help create and publish material. Each entry in a blog can be commented upon, which provides opportunities for discussion and can help generate new ideas.

Blogs are hosted by dedicated blog hosting services or regular web-hosting services and today hosting service fees are considered reasonably priced.

1. https://en.wikipedia.org/wiki/Blog

Moblogs

Mobile blogs, known as moblogs, are a method of publishing onto a website or blog using a mobile phone or handheld device. Moblogging[2] emerged thanks to the development of e-mail features in mobile phones (see Fact sheet 5 on mobile technology).

Vlogs

A video blog or video log is the same as a blog, described above, but the postings are in video format. Vlogs were initially popular on YouTube, and now you can find vlogs on Vine, Instagram, Facebook and even Pinterest.

RSS feeds

RSS[3] or rich site summary is now being used to syndicate blogs. Those who wish to have their content published on other websites can make it available using an XML[4] or extensible mark-up language version for Web syndication.

XML is a type of code similar to HTML and is also known as a "feed". Basically it allows readers to "subscribe" to content and have blog updates delivered to them so that they do not have to visit the blog to get it.

Educational importance of blogs and vlogs

► Blogs and vlogs provide their creators with a voice. Bloggers and vloggers are able to share their interests, exchange their thoughts, and inform their audience on issues that resonate for them. They are able to document life, to share adventures and to provide visual viewpoints on a platform easily accessible for all.

► Bloggers and vloggers can simultaneously be mobloggers as they use their smartphones to write, publish and upload content.

► As smartphones are widely available, a more diverse and often younger audience is able to blog and vlog, without the necessity of expensive computing hardware.

► Blogs and vlogs are also used by journalists, researchers and activists as an important means and source of information and expression.

► There has also been the development of blogs and vlogs focusing on disability and special needs to provide awareness and start discussion.

Blogs in the educational environment

Blogs give students a chance to take control of their learning and set up a public forum in which to publish their thoughts and feelings, and they can be used as a creative teaching tool for discussion and collaboration. For example, a modern literature class used blogging to study the novel *The secret life of bees*. The author wrote an introduction to the lesson and students and their parents were invited to write about their impressions of each day's reading assignment. The author then commented on these (see <*http://techtraining.dpsk12.org/ilt/Bees/SLOBees.pdf*>).

Experts note a three-step process involved when blogging: defining audience, purpose and scope. This is described on the website <*https://macln.wordpress.com/2011/01/12/three-step-process-for-blogging/*> . Bloggers must continually scour, filter and post material. By searching for material to comment on, the student becomes increasingly familiar with different theories and ideas and develops the skills needed to critically analyse content and to discern truthful content.

Technology can be used as a motivating factor in education. Students are interested in blogs because of their creativity and possibilities for self-expression. This can be used as a vehicle to teach a wide variety of subject matter.

Blogs give every student in the class a chance to participate in a discussion, which exposes children and young people to different perspectives.

2. https://en.wikipedia.org/wiki/Mobile_blogging
3. https://en.wikipedia.org/wiki/RSS
4. https://en.wikipedia.org/wiki/XML

ETHICAL CONSIDERATIONS AND RISKS

- Remind students that they should not give out personal information in public Internet spaces that they would not disclose in an offline forum. This is a particular problem with blogs, which are often personal by their very nature.

- Even anonymous blogging is not always completely anonymous and taking down a blog does not necessarily remove all contents from view.

- Think about your security offline and ask the question: how easy would it be for someone to find me based on the information I have provided?

- Consider the voice and personality that you are going to use as a blogger or vlogger. Would this be considered offensive to some? Would this be considered offensive to your school or future employer?

- Blogs and vlogs can also be used to disseminate hateful and discriminatory messages or to promote extreme, radical or disturbing content.

HOW TO

If you have the technical skills, you can create a blog from scratch. Most people use sites which offer tools for creating and publishing content as a blog. School Blogs at *<http://www.schoolblogs. net/wpress/>*, Blogger (see below) and Wordpress are popular hosts which provide free services. They provide easy, step-by-step instructions, which help you create an account, name your blog and choose a template.

Once your blog is up and running, you compose and edit entries from a central webpage. The interface for popular software is WYSIWYG[5] format and is extremely user-friendly. Visitors to your blog can comment on content by clicking on a comments link at the end of each entry.

You can choose to moderate your comments before they are displayed on your webpage.

Be sure to enrich your commentary with hyperlinks and images. Buttons for these features should be included on the toolbar above the text box where you enter your content.

IDEAS FOR CLASSROOM WORK

- Have students divide into teams of two where one student is the blogger and the other student is the interviewee for the subject. The journalist blogger conducts an interview and then writes a blog for the interviewee to approve.

- Research the top blogs and vlogs dedicated to disability, special needs, social change or social awareness. Invite students to discuss how they can contribute by commentary or submitting a blog post.

- Have students consider what is the best method to convey their message: blog, vlog, a series of tweets, Vine videos or Periscope videos. The sky is the limit. If the students choose Twitter, Vine, Periscope or another app, remind them to include links to their blog.

- Ask the student to list 5-10 topics of interest. Then do some research to find out if blogs exist on their preferred subject matter.

- Research some of the top student and young people bloggers. What subjects do they address: the environment, politics, fashion, music, technology?

---

5. "What You See Is What You Get": https://en.wikipedia.org/wiki/WYSIWYG

- A blog is a great opportunity to air your views but you may wish to protect your privacy by using a pseudonym and holding back certain personal details. Children and young people should be particularly careful about revealing personal information in a blog.

- Respect copyright laws and do not use other people's blog designs or photos within a blog without their permission. There are many websites that allow you to use their photos for free with or without attribution.

- Start your own blog to familiarise yourself with the practice before introducing it into the classroom. It might help to visit other blogs for ideas and inspiration. The School Blogs[6] website has more than 4 000 members and gives users the possibility to launch their own school blog.

- Spend time explaining the concept of blogging to your students. Tell them why it is done and give examples of good and bad blogs. Then give students a set of strict rules which might include length and frequency of posts, topics, number of hyperlinks/photos and so forth. Ask students to keep a blog, discuss their experiences and comment on others' blogs.

FURTHER INFORMATION

- Blogger is a site providing tools for blogging and now moblogging: *<www.blogger.com/start>*.

- Legal and ethical tips for bloggers can be found at: *<http://weblogs.about.com/od/bloggingethics/tp/Blogging-Best-Practices.htm>*.

- Electronic Frontiers Foundation (EFF) offers a legal guide for bloggers: *<http://www.eff.org/bloggers/lg/>*.

- Weblogg-ed – this site follows current blogging trends in education: *<www.weblogg-ed.com/>*.

- "Blogging and RSS – the 'what's it?' and 'how to' of powerful new Web tools for educators": *<http://web.archive.org/web/20160413030845/http://www.infotoday.com/MMSchools/jan04/richardson.shtml>*.

- "The educated blogger: using weblogs to promote literacy in the classroom": *<http://firstmonday.org/ojs/index.php/fm/article/view/1156/1076>*.

- Tools to support K-12 student writing can found at *<www.readwritethink.org/student_mat/index.asp>*.

- Blogging resources for educators are available at *<http://www.socialstudiescentral.com/>*.

- Darren Rowse was one of the first bloggers to make a living entirely from blogging. He provides tips and resources on his website: *<www.problogger.net/>*.

- Websites with free photos for use on blogs include *<www.pixabay.com>*, *<www.flickr.com/creativecommons/>*, and *<www.freedigitalphotos.net>*.

- "Learning together to be safe", a toolkit developed for schools by the UK Department for Children, Schools and Families, provides resources for teachers on issues such as extremism and radicalisation: *<www.preventforschools.org/download/file/mmu-learning-together-to-be-safe.pdf>*.

- Relevant Council of Europe articles, including the European Convention on Human Rights *<www.echr.coe.int/Documents/Convention_ENG.pdf>*:

  Article 8 – Right to respect for private and family life.

  Article 10 – Freedom of expression.

---

6. http://www.schoolblogs.net/

- Relevant UN Convention on the Rights of the Child articles:

  Article 13 – Children have the right to get and to share information as long as the information is not damaging to them or to others.

  Article 16 – Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

  Article 29 – Education should develop each child's personality and talents to the full. It should encourage children to respect their parents, and their own and other cultures.

Internet on the Go

T he use of the Internet on the Go – using the Internet on a portable computer or handheld device via mobile or wireless connection – is on the rise as individuals take advantage of new ways to connect when they are away from home or work.

▬ In 2012, 36% of people aged 16 to 74 within the EU-28 used a mobile device to connect to the Internet. Two years later, the number had risen to 51%. Studies[1] show that the most common mobile devices for Internet connections were mobile or smart phones, laptops, notebooks, netbooks or tablet computers.

▬ Few people bought mobile phones when they first became available in 1983. In 1995, there were five mobile subscriptions per 100 inhabitants in the European Union. According to Eurostat, in 2003 the figure was 80 mobile phones per 100 inhabitants among the enlarged EU of 25 countries.

▬ Ten years later, the number of smartphone subscriptions was around 400 million, representing almost 40% of total handsets. By the end of 2020, Ericsson forecasts the number of smartphones in Europe to reach 800 million[2].

1. http://web.archive.org/web/20160413105315/http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals
2. http://web.archive.org/web/20150324081657/http://www.ericsson.com/res/docs/2014/emr-november2014-regional-appendices-europe.pdf

▬▬ The lines between mobile technology and personal computing have become blurred as most mobile phones have Internet browsing and e-mail capabilities, and more computers are wireless.

MOBILE TECHNOLOGY

▬▬ Mobile technology is the technology used for cellular communications and some argue that mobile technology is the future of computing[3].

SMS

▬▬ Short message services (SMS) is the text messaging service feature of phone, Web, or mobile communication systems[4].

MMS

▬▬ Multimedia message services (MMS) is a feature which allows users to send messages that include multimedia content to and from mobile phones[5].

M-learning

▬▬ Mobile learning or m-learning refers to learning with the aid of mobile technologies, such as mobile phones, handheld computers and personal digital assistants (PDAs)[6].

Geolocation

▬▬ Geolocation is the ability to identify an object's real-world geographic location, such as a mobile phone or Internet-connected computer terminal.

▬▬ Mobile technology users should understand the geolocation function on their devices and be able to set standard privacy settings on mobile devices (for more information on privacy settings, see Fact sheet 9).

Apps

▬▬ A mobile application or app is a computer program specifically designed to run on mobile devices such as smartphones, tablet computers, smart watches and in some cases, wearables[7]. For more information on wearables, see Fact sheet 23.

▬▬ The amount of apps has increased in direct proportion to the amount of mobile phone users and the app economy is estimated to create revenues of more than €10 billion per year within the European Union[8].

▬▬ There is a huge variety of apps available that are either free or paid and it is advisable to read the reviews on apps before download or purchase because free apps can finish up being costly through in-app purchases (see Fact sheet 13 on online shopping).

Mobicash

▬▬ With the increase in mobile phone users, financial institutions have introduced a single cashless mobile financial platform, which offers transaction processing and mobile payments.

▬▬ "Orange money", for example, which describes mobile money services from the provider Orange, is available in 13 countries: Botswana, Cameroon, Cote d'Ivoire, Egypt (under the name Mobicash), Guinea, Jordan, Kenya, Madagascar, Mali, Mauritius, Niger, Senegal and Uganda[9].

▬▬ UK reports British consumers are likely to spend as much as $30.5 billion by 2021 on purchases through their mobile handsets[10].

---

3. https://en.wikipedia.org/wiki/Mobile_technology
4. https://en.wikipedia.org/wiki/Short_Message_Service
5. https://en.wikipedia.org/wiki/Multimedia_Messaging_Service
6. https://en.wikipedia.org/wiki/M-learning
7. https://en.wikipedia.org/wiki/Mobile_app
8. http://web.archive.org/web/20160617033122/http://www.visionmobile.com/product/the-european-app-economy/
9. https://goo.gl/4LQveU
10. https://goo.gl/8a7Dx7

IMPORTANCE IN UNDERSTANDING THE ISSUES

- There are concerns about children receiving mobiles or tablets too early, as long-term research has not yet been carried out to investigate what developmental issues can be posed by early access to mobiles or tablets.

- Additional concerns for children include online shopping and engagement in e-commerce without understanding the implications.

- Research is inconclusive about the dangers of radiation exposure over time, however minimal this may be.

- Although computer use is often still regulated within the home, many parents consider that mobile phone use is "private". Emboldened by newfound freedom, children can get themselves into financial trouble by spending money on prize "giveaway" media campaigns or accessories such as ringtones.

- Mobiles may be used as tracking devices through the geolocation facilities they contain. The issue of safety versus freedom is a controversial one.

- Bluetooth technology[11] raises security issues such as hacking, and sending or receiving unsolicited messages.

- Moblogs[12] are mobile phone blogs (web diaries). They make it easy for young people to post information and photos and potentially compromise their own safety and that of others.

- Mobile bullying is of growing concern and is not only limited to smartphones and tablets, as smartwatches now exist with social networking apps pre-installed.

- Mobile phone cameras and easy Internet access capabilities can be a threat to privacy: there is a worrying trend amongst young people to take "compromising photos" (e.g. other young people in the gym changing room or in embarrassing situations, teachers in class), and even the morphing of these images before they are uploaded to the Web.

- Mobile phone costs: children are often unaware of the high costs of certain services, such as online voting, unwanted premium SMS services and in-app purchases.

- Because they are a distraction, mobiles can pose a risk while driving and, even more recently, they have been noted to pose risks when walking. So many individuals walk and text that there are even apps that allow you to see the ground as you text with your head down. Available on Apple[13] or Android[14].

- Viruses[15] have been infecting mobiles since they became a household item, around 2004. F-Secure estimates that hundreds of mobile viruses exist and they are increasing in type and number all the time. Take a look at the most recent threats at "Threat descriptions"[16].

ETHICAL CONSIDERATIONS AND RISKS

- Internet "on the go" poses several risks because many do not give a thought to using appropriate privacy settings. The facility of use and availability of several devices per user make intrusions more likely.

- Many users take advantage of free wireless connectivity available in cafés, restaurants and other public locations and provide personal and financial information in these environments.

---

11. https://en.wikipedia.org/wiki/Bluetooth
12. https://en.wikipedia.org/wiki/Mobile_blogging
13. https://itunes.apple.com/en/app/type-n-walk/id331043123?mt=8
14. https://play.google.com/store/apps/details?id=com.biztech.typewhilewalk&hl=en
15. http://en.wikipedia.org/wiki/Computer_virus; https://en.wikipedia.org/wiki/Mobile_virus and worms; http://en.wikipedia.org/wiki/Computer_worm
16. https://www.f-secure.com/en/web/labs_global/threat-descriptions

- Internet, anytime, anywhere, also means that there is no cool-off period for making decisions about what to upload or post online, about online purchases and other online activities. For instance, many apps allow live-streaming of events as they happen so your child may stream an embarrassing or violent scene unfolding in front of his/her eyes without being able to reflect on whether it is a good idea or not to record or publish such content.
- Due to the ease at which even very young children can make purchases via mobile devices, specialists warn of an emerging trend of what they call "virtualisation" of money, where children have difficulty grasping the real value of money.

HOW TO

Mobile phones are popular and it is easy and relatively inexpensive to own one. Once you buy a handset you can choose to pay à la carte for certain increments of minutes or you can subscribe to a specific provider and pay a monthly fee for services.

Mobile devices such as smartphones, tablets, eReaders and hand-held games only require a Wi-Fi connection to provide access to the online world.

IDEAS FOR CLASSROOM WORK

Since mobile phones are so popular with young people, teachers can engage students by incorporating the use of SMSs and so forth in classroom activities. The portability of handheld devices is beneficial for teachers who are on the move and for students working in groups or doing fieldwork. The use of mobile devices in learning both in school and out has been found to encourage students to take responsibility for their work and to make it less likely that they lose notes and assignments.

- While on a field trip, have students record their impressions on a mobile device, using photos and videos to supplement their assignments.
- Have students use various apps to detail their homework, for example Vine for short videos, Periscope for on-the-spot reporting, or Twitter and Facebook for academic updates.
- Ask students to identify the risks and challenges of using smartphones and mobile devices in the classroom. Do they think that a 100% tech classroom is possible? Why? Why not?

GOOD PRACTICE

- Use a low-radiation mobile phone[17], that is an ear SAR rating of no more than 0.56 W/kg and a body SAR rating of less than 0.57 W/kg, and a head-set – the best ones are equipped with a frequency filter.
- Encourage young people to restrict their use of mobile phones and tablets. Do not prohibit use, however. Mobile phone use and various messaging services are a widespread phenomenon among teens and in many circles it is essential for networking among peers.
- Do not leave Bluetooth on if it is not being used, in order to avoid security risks.
- As with e-mail, accept data only from trusted sources. Beware of SMS spam: only share your mobile number with people you know well.
- Before publishing pictures, make sure they will not breach the legal rights of others.
- Talk to your children about exchange of harmful content and stress that it could be against national youth protection laws.
- Be considerate with your use of the phone and tablet. People around you may not appreciate having to listen to your conversation.

17. http://www.phonerated.com/top-rated-best-overall-low-sar-phones-global

- If you are bothered by unwanted calls or SMSs, contact your mobile operator or your national Insafe helpline[18].

- Many mobile phones have a filter option: use a black list to block unwanted numbers or a white list to only accept elected numbers (for example only numbers in the address book). You can also download parental control filters from the Internet (freeware) or buy one from your mobile operator.

- Remember that mobile phones are not the only devices that can be used to communicate: tablets and smart watches also have messaging and voice capabilities.

- For younger children, or teens who are not yet able to manage their finances responsibly, choose a "pre-paid" plan instead of a monthly subscription in order to avoid unpleasant surprises. Discuss their spending and ensure that they understand the real value of money.

- Do not forget to configure your child's smartphone upon purchase. Most devices come with fully fledged features (camera, GPS, near field communication (NFC), Bluetooth, etc.) and are configured by default for adults. Do not hesitate to search for online guides on setting up your child's smartphone. Some of the steps recommended are: set up a child's account protected with a password, disable in-app purchases, disable installation of new apps (for very young children), disable geolocalisation and the use of GPS and install parental control software.

- Beware that once a password is entered to make a purchase on a mobile device, the password may remain active for up to 15 minutes allowing another purchase to be inadvertently made[19].
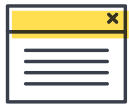
FURTHER INFORMATION

- A GSMA report can help understand the mobile economy: *<http://web.archive.org/web/20160411155639/http://www.gsmamobileeconomy.com/GSMA_Global_Mobile_Economy_Report_2015.pdf>*.

- Europe's social, digital and mobile landscape in 2014 gives a range of infographics: *<http://web.archive.org/web/20151211195326/http://wearesocial.net/blog/2014/02/social-digital-mobile-europe-2014/>*.

- S212 is an independent UK site for reviewing mobile phones and other devices: *<http://www.s21.com/mobile-phones.htm>*.

- UNESCO has published a report on the future of mobile learning and its implication for policy makers and planners: *<http://unesdoc.unesco.org/images/0021/002196/219637E.pdf>*.

- "Children and mobile phones, an agenda for action" is an online publication by Childnet International: *<http://www.childnet.com/ufiles/CMPAAA_A4.pdf>*.

- The British Board of Film Classification has taken over from the Independent Mobile Classification Body (IMCB) to provide the independent framework that underpins the mobile operators' code of practice: *<http://www.bbfc.co.uk/what-classification/mobile-content>*.

- Learn about protecting Bluetooth and how it works: *<http://web.archive.org/web/20160407133222/http://electronics.howstuffworks.com/bluetooth4.htm>*.

- Mobile operator Vodafone has written a guide for parents: *<https://www.vodafone.com/content/parents/howto-guides.html>*.

---

18. http://www.saferinternet.org/ww/en/pub/insafe/focus/national_helplines.htm
19. http://www.creditcards.com/credit-card-news/whos-responsible-kids-unauthorized-charges-1279.php

2. Internet – Connecting ideas and people

> ❝❝ "Eventually everything connects – people, ideas, objects. The quality of the connections is the key to quality per se."
>
> *Charles Eames, early 20th century designer*

CHECKLIST FACT SHEET 6 – E-MAIL AND COMMUNICATION

Have you created several e-mail accounts and set different passwords for each?

Is the password sufficiently "strong" (more than 8 characters long, with a combination of letters, numbers and symbols)?

Do you clearly label your e-mails with relevant key words in the subject line?

Have you enabled two-factor security on your e-mail accounts (providing an extra security question and/or your mobile phone number)?

CHECKLIST FACT SHEET 7 – CHAT AND MESSAGING MEDIA

Have you included contact details in your website or blog?

Have you taken steps to protect your online privacy?

Have you checked that the content that you are using for your website/blog is in accordance with copyright law?

CHECKLIST FACT SHEET 8 – SOCIAL NETWORKING AND SOCIAL SHARING

Reputation is something we only have one of: do you systematically "think before you post"?

When did you last update your privacy settings on the sites you use?

Democracy depends on the participation of as many citizens as possible in the public debate: have you tried making your voice heard through relevant social network sites?

CHECKLIST FACT SHEET 9 – PRIVACY AND PRIVACY SETTINGS

Is it necessary to post that tagged photo on a social networking site?

Have you read the mobile app agreement to understand what are you sharing: what you own and what "they" own?

When you upload apps, are you sure you know exactly what private information they will access? Is such access really necessary for the app to function?

Do you understand what the European Union's General Data Protection Regulation implies for you?

E-mail and communication

Email[1], short for electronic mail, is the system for sending messages between computers connected in a network such as the Internet. The term also refers to the message itself. An e-mail is usually transferred successfully in a matter of seconds and the recipient can access and reply whenever it is convenient. A flexible and efficient system, e-mail has drastically changed the way we work and communicate. Billions of messages are sent every day.

An e-mail address is composed of two parts: local and domain names, separated by the "@" sign. The local name will often – but not always – indicate the name of a user. The domain may indicate the user's organisation, company or Internet service provider. Domain names may also indicate the type of organisation and/or country. For example, name@ox.ac.uk would be someone working or studying at Oxford University.

Although many other ways of communicating have emerged, e-mail accounts are still at the heart of a user's online experience since it is often the only way to create accounts to participate online. So, while other means of communicating may now be preferred to e-mails (social networking, instant messaging, etc.), e-mails have become the "key" to the online identity of users, serving often as a "login" to connect to all the online services they use.

---

1. https://en.wikipedia.org/wiki/Email

IMPORTANT IN EDUCATION

IMPORTANCE IN EDUCATION

Because e-mail addresses are so often asked for online, learning to manage an e-mail account properly carries a lot of educational value, much like learning to sort physical mail by classifying the personal content and the important administrative content in order to find it easily.

E-mail is also a valuable tool in cross-cultural projects between classes of children and young people in different countries. Children and young people can use it to develop their language skills and share information about their cultures.

Some of the more reserved children and young people may express themselves better through e-mail than they would in face-to-face classroom discussion.

ETHICAL CONSIDERATIONS AND RISKS

- Because your e-mail is the "gateway" to all your online accounts, the consequences of someone breaking into your e-mail account can be very serious.

- Most e-mail clients (computer programs used to access and manage a user's e-mail[2] you can find online are free, but many of them use algorithms to scan the content of your e-mails and display targeted advertising on the webmail page.

- The expression of emotions via e-mail is difficult. This is why you should always write your messages with care to make sure they are not misunderstood. "Emoticons"[3], small expressive icons such as smiley faces, can help you express your intentions, especially irony or humour. Use these sparingly, however, to keep from distracting from your message.

- A high proportion of e-mail received is unsolicited and usually undesired spam[4] (see Fact sheet 19 on spam, malware, fraud and security). Fortunately, spam filters are getting increasingly better at sorting spam from regular e-mails.

- Be sure not to contribute yourself to "spamming" by abusively forwarding e-mails that you find "funny" or "interesting" to all of your contacts. If you do so too often, spam filters may identify your e-mail address as a proxy for spam and blacklist it, making it impossible for you to contact anyone.

- Some "forwards" are false or fraudulent. An example are e-mails that falsely claim that a company or organisation has promised to pay a small sum of money for a humanitarian cause (often citing a cause such as a sick child requiring surgery) each time the mail is forwarded.

- It is easy to conceal a name in order to be misleading. This can be done by simply changing the name in the settings or creating a webmail address such as *elvispresley@hotmail.com*. Even if you recognise the e-mail address as belonging to one of your contacts, check the subject line too because it is possible that that the owner's machine may have become a "zombie computer"[5] affected by a hacker or virus.

- A link may appear to be directing you to one website when in fact it leads to another. This is particularly common in phishing scams[6].

2. https://en.wikipedia.org/wiki/Email_client
3. https://en.wikipedia.org/wiki/Emoticon#Basic_examples
4. https://en.wikipedia.org/wiki/Email_spam>
5. https://en.wikipedia.org/wiki/Zombie_(computer_science)
6. https://en.wikipedia.org/wiki/Phishing

- Create several e-mail accounts for different purposes (signing up to social networking sites, purchasing products online, etc.). Keep one account as private as possible by not publishing it on the Web and using it solely for important services you and your friends use. Use a different one to sign up to services you might only use once, or services that you rarely use.

- Keep e-mail messages short and to the point. Try to avoid long blocks of text. Check your spelling.

- Make sure you include relevant words in the subject line. This helps the recipient identify your message as being genuine and helps to find the e-mail at a later time.

- Create strong passwords for your e-mail accounts (more than 8 characters long, combining letters, numbers and symbols) and use different passwords for each account.

- Be considerate in the volume of e-mail you send out and be smart and strategic about how you communicate with others. If you need to have a group discussion with a large number of people, perhaps it is more useful to organise a conference call or a chat on a private forum rather than sending a massive amount of e-mails.

- Avoid checking your e-mails every 10 minutes. Many people allow e-mail to be a constant interruption.

- As a general rule, never include sensitive information in an e-mail, such as bank details. There are only rare circumstances where you will need to send such information, for instance, to make a hotel reservation. In case of doubt, proceed with caution, check the online reputation of the service you want to use, check the procedure to cancel your card or the transaction, use more secure payment services, such as PayPal, and avoid less secure services, such as direct money transfer services (e.g. Western Union). However, never send details such as your username and password of your online accounts via e-mail. Online services will never ask you for this, so if you receive an e-mail asking for such details, it is definitely a phishing attempt.

- More and more sophisticated phishing strategies consist in "false" notification e-mails that emulate perfectly the messages you receive from the services you use (social networking sites) and send you to a false website that asks for your username and password to log in. Make sure that you always check the e-mail address of the sender and the address of the website for anything unusual.

- Maintain a healthy scepticism about e-mails you receive. Do not open e-mails if you do not trust the source.

- Be especially wary of attachments. If you were not expecting an attachment from the sender or do not trust it for any other reason, delete without opening. Even attachments from known and trusted senders should be first saved then scanned before opening.

- Make use of all the security features that your e-mail client proposes. Usually, e-mail clients enable you to enter a secondary email address in case that e-mail account gets hacked and, increasingly, e-mail clients propose that you enter your mobile phone number for extra security checks in exceptional circumstances. If your account is compromised, configure your security settings properly so it will be much easier for you to recover it.

- Be sure to consult Fact sheet 19 on spam, malware, fraud and security for additional advice on e-mail.

- To consult your e-mails, you can either use the "official" app of the e-mail service on your smartphone, tablet or even your computer running Windows 8 or above (such as the Gmail app, the Outlook app or the Yahoo! app), you can go to the website of the e-mail service (using a "web-

mail" service) or you can use an email client which is an external application that downloads your e-mails from your e-mail service and enables you to manage/organise them. The "up" side of using an e-mail client is that you can configure it to download e-mails from several different e-mail services so you can consult all of your e-mails from your different e-mail addresses in one place. The most popular e-mail clients are Thunderbird and Outlook. E-mail clients are mostly used for professional e-mail.

- For information on setting up a spam filter see Fact sheet 19 on spam, malware, fraud and security.

IDEAS FOR CLASSROOM WORK

- For older students that have an e-mail address, ask them to connect to their e-mail service and explore the security settings in order to secure their e-mail account by adding an additional security question, a second e-mail or a mobile phone number.

- Here are the procedures to follow to secure your e-mail account for Gmail, Yahoo! and Outlook.
    - ▶ *<https://support.google.com/accounts/answer/46526?hl=en>*
    - ▶ *<http://windows.microsoft.com/en-us/windows/outlook-security>*
    - ▶ *<https://help.yahoo.com/kb/SLN8292.html>*

- There are many e-mail providers out there besides the three "big" ones above. Why insist on those three? Because, at least for Gmail and Outlook/Hotmail, they are linked to many other services. For instance, a "Google" account is almost a necessity when you own an Android smartphone and an Outlook account is often linked to your Windows operating system. This means that, regardless of your preferences, you might be "forced" to create an e-mail account on one of the services above. But you are of course free to use e-mail clients with higher privacy standards such as Web.de or Protonmail.com. Even your Internet service provider usually offers an e-mail service. Feel free to search for other alternatives online.

- Get your students to work in teams of three or more and ask them to make up good passwords for an imaginary e-mail account. Be very clear that they should not share their real password! After a 10-minute brainstorming, ask each team to present their proposed password and why they think it is secure. Help them identify the characteristics of a strong password (more than 8 characters long, combining letters, numbers and symbol characters) and the common pitfalls of weak passwords (can be found in a dictionary, is related to you in some way – name of dog, family name, etc.).
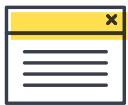
FURTHER INFORMATION

- Well-known examples of e-mail clients are Microsoft Outlook *<https://products.office.com/en-us/outlook/email-and-calendar-software-microsoft-outlook>* or Mozilla Thunderbird *<http://www.mozilla.org/projects/thunderbird/>*.

- Truth or Fiction is a website for Internet users to check the veracity of commonly forwarded e-mails *<http://www.truthorfiction.com/>*. Another similar website is *<http://m.snopes.com/whats-new/>*.

- Three of the most popular webmail sites are Outlook *<https://office.live.com/start/Outlook.aspx>*, Yahoo! *<https://mail.yahoo.com>* and Google's Gmail *<http://www.gmail.com>*. Feel free to search for alternative e-mail providers, especially in your country.

- Relevant UN Convention on the Rights of the Child articles:

    Article 13 – Children have the right to get and to share information as long as the information is not damaging to them or to others.

    Article 16 – Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

Chat and messaging media

▬▬ "Chat" is a generic term that refers to interactive communication which takes place on a dedicated discussion channel. Users can talk to groups of people in chatrooms[1] or hold private conversations with selected friends by using instant messaging[2] services.

▬▬ Chatting is a very informal means of communication, similar to face-to-face conversations, and occurs between two or more people. Chat discussions are usually typed but can also include video or audio streaming[3] through the use of headsets or webcams. This form of communication is instantaneous and therefore different from e-mail, which does not depend on the recipient being present at the same time as the sender.

Chatting vs. instant messaging

▬▬ The terms are used interchangeably; however, a user can chat while using instant messaging services, but sending an instant message (IM) is not a chat. Chat used to be quite popular but seems to be losing its position to instant messaging and other types of messaging media. Many companies

1. https://simple.wikipedia.org/wiki/Chat_room
2. https://en.wikipedia.org/wiki/Instant_messaging
3. https://en.wikipedia.org/wiki/Streaming_media

frown upon IM in the work environment as it tends to reduce productivity if employees are constantly interrupted by messages while performing their tasks.

What are other types of messaging media?

▬ Messaging apps such as WhatsApp, Kik, Viber, Telegram or iMessage are increasingly being used by smartphone owners. Auto-deleting apps such as Snapchat and Wickr are also popular with smartphone owners. These types of messaging media are typically free and seemingly offer more "privacy" than the types of messaging that are available on larger platforms such as Facebook, Twitter or LinkedIn.

▬ The quick availability of these messaging apps on smartphones often means that users film, comment, take photos and send before thinking of the ramifications. They have therefore, unfortunately, been cited as playing a part in the increase in online harassment and bullying.

▬ The growth of instant messaging and other types of messaging media will undoubtedly continue as smartphones are entering new markets. Facebook has acquired WhatsApp, the Japanese company Rakuten purchased Viber and many of the other messaging apps have been injected with investment money from interested parties. The message could not be clearer: messaging media will be around for a while.

Importance in understanding chat and instant messaging

▬ Chat and instant messaging are popular pastimes and are transforming the way young people communicate with each other. Chatting and instant messaging are used in positive ways as students exchange ideas and discuss homework and other academic projects, but they are unfortunately also used to bully and harass others online (see Fact sheet 21 on bullying and harassment).

▬ Teachers often underestimate how important chat is to young people and may miss the opportunity to harness this force and apply it as an educational tool. Some ideas include:

· brainstorming sessions and problem-centred real time discussions

· role-playing games and simulations

· exchange of opinions and debates and small-group panel discussions

· tutoring and guidance

· group investigation

· creation of an online community.

⚠ ETHICAL CONSIDERATIONS AND RISKS

· When chat is text based, social cues, gestures and non-verbal communication cannot be transmitted through typing, and misunderstandings can easily occur online. One should be as agreeable, polite and well-mannered as in real-life situations and make a habit of using good netiquette[4]. Humour and emotions can also be shown through use of emoticons[5], small symbols that look like faces written sideways. Most young people use linguistic shortcuts or acronyms, and you can find a dictionary of the most common of these at <*http://www.netlingo.com/acronyms.php*>.

· When chatting with strangers on the Web, it is also important to remember that people are not always who or what they say they are. Closed groupware chats[6] that provide conferencing possibilities for use in a school or classroom setting are safer to use because access is limited to a defined user group.

· The time spent chatting or sending IM has greatly increased with teenagers sending hundreds of messages in various forms (texts, IM, chats, e-mails, etc.) every day. While the ergonomics of computer keyboards and computer mice have greatly improved, new syndromes such as

---

4. https://en.wikipedia.org/wiki/Etiquette_in_technology#Netiquette
5. https://en.wikipedia.org/wiki/Emoticon
6. https://en.wikipedia.org/wiki/Collaborative_software

"teenage texting tendonitis" have appeared. Smartphones are relatively recent devices, and sending messages or typing long e-mails may result in overuse of the thumbs. Limiting chat and texting is therefore not just a life-balance issue but also a health issue.

- While many IM apps appear to be "free", always keep in mind that a company has to cover its operating costs one way or another. Many apps opt for a "build and sell" strategy, attracting users with a "free" app, and then sell the user base to another company as soon as it is large enough. Such was the case with Whatsapp which was bought by Facebook. Other apps such as Snapchat first build their user base and then start introducing advertising. Always be aware of the business model of the IM service you are using and choose wisely, taking into consideration the trade-offs (less privacy, control over your data, exposure to advertising, yearly/monthly fee, etc.).

- People often exchange files through messaging and chat, and it is important to remember that files can contain malware. Make sure that all files have been scanned for viruses before sharing them and scan anything you receive before opening it (see Fact sheet 19 on security).

- There has been a lot of negative publicity about the risks young people might encounter when using chatrooms. Due to several high-profile criminal cases, parents and teachers often worry about the possibility of children coming into contact with paedophiles in chatrooms, especially through online games (see Fact sheet 16 on games). Although these dangers do exist, it is important to keep these fears in perspective. A vast majority of chatroom users are who they say they are, and most chat communication is completely innocent. Rather than preaching fear or banning the use of chat, adults should empower the young by teaching them how to stay safe. Here are some basic rules that children and young people should follow:

  ► Choose a chatroom appropriate to your age group and with a live moderator, and report any negative incidents to the moderator.

  ► Use a gender-neutral user name and never give out your personal information or post photos of yourself (see Fact sheet 9 on privacy).

  ► If you are really going to meet a chatroom friend, discuss it first with your parents and take a trusted adult along with you. Always meet up in a public place, such as a town square, on the first physical meeting with someone you met online.

  ► Tell an adult if anything you have encountered in a chat session makes you feel uncomfortable. If you encounter any problems in a chatroom or anywhere else on the Internet you can always discuss it with experienced advisors at your national helpline[7].

  ► If you want to chat with people you know, consider using instant messaging (e.g. MSN, Skype) instead of a chat room so that you can control your contact list.

HOW TO

- There are many kinds of free chat programmes available on the Web. You can find a wide range by searching for "chat" in any search engine[8]. Many web-based chat programs, such as Yahoo Chat[9], ICQ[10] and AOL Chat[11] provide a wide variety of chatrooms with real-time discussion groups. Users must often first download a small application to enable chat and register with the moderator but can then login and participate freely.

- Instant messaging[12] applications, which allow private conversations with selected users, now surpass chatrooms in popularity. These capabilities can be found by searching for "instant messaging" in any search engine. Users download an application to enable instant messaging and then compile a list of people with whom they want to chat. Because communication takes place in a restricted user group, instant messaging is often considered "safer" than chatting in chatrooms.

---

7. www.betterinternetforkids.eu/web/portal/practice/helplines
8. https://en.wikipedia.org/wiki/Web_search_engine
9. http://chat.yahoo.com
10. http://www.icq.com/
11. http://lifestream.aol.com
12. https://en.wikipedia.org/wiki/Instant_messaging

How to use a chatroom?

- Open the chat program that you have chosen to use.
- Provide a username and password, if necessary.
- Choose an appropriate, humanly-moderated chatroom. Usually there are rooms for different purposes and topics, for example automotive interest groups, subject-specific study groups, chats for teachers and so forth.
- Once you are logged in, you will see the participants' conversation scrolling on the main text screen.
- Type your message and press "enter" or click "send" to post it so participants can see it.
- If you want to send a message to one specific person, select a person from the participant list in the window.
- Many chatrooms can also be used for peer-to-peer[13] file exchange. Chatrooms enable the swapping of files too large to be sent by e-mail[14].
- Always check your settings so that you do not inadvertently add unwanted users to your chatroom.

How to use instant messaging?

- Open your instant messaging application[15].
- Check your list of contacts to find out who is online and available to chat.
- You can add new contacts by entering their e-mail address and inviting them to join your contact group. They will receive an e-mail invitation and, if they agree, will be registered in your list. This will enable you to chat with them real-time when you are both online.
- Click on the selected person's ID to send a message and open a dialogue for communication.
- Type your message and press "enter" or click "send" to post it so participants can see it.
- It is best not to engage in conversations with unknown users or respond to e-mail or IM from people that you do not know.
- Always check your settings so you do not inadvertently add unwanted users to your IM.

IDEAS FOR CLASSROOM WORK

- Pick a topic and have students ask each other questions and exchange information in a chat setting.

- Decide on a study topic. Gather some orientation material to help students to do their pre-lesson activities. Have the students work on their assignments in pairs or small groups. This working phase should be organised along the lines of a group study model (chat works at its best in small-group interactions, that is 2-6 students).

- At the end of the project, students prepare presentations suitable for a chat session. Chat starts with small-group presentations of different study topics. The study community sums up together what they have learned during the course.

- Because chat sessions model real-life conversations, they offer students opportunities for authentic interaction and are therefore useful in studying foreign languages. The teacher can encourage students to participate in the discussion, advising them to post short messages. Interaction can be enhanced by creating roles for students: one may be an innovator, another a critic. The other students can follow the discussions and later provide feedback.

- Environment Online (ENO)[16] is an international web-based environmental education project. At the beginning of the course, students get their topics from the web pages of the project. The students collect scientific and empirical environmental data, measure different phenomena or take photographs.

---

13. https://en.wikipedia.org/wiki/Peer-to-peer
14. https://en.wikipedia.org/wiki/Email
15. https://en.wikipedia.org/wiki/Instant_messaging
16. http://www.enoprogramme.org

- During each theme period, virtual lessons are arranged in the form of interactive and synchronous real-time chats[17], electronic questionnaires and message boards[18]. Before and after lesson activities, students share ideas, monitor their tasks via chat and reflect on what they have learned.

GOOD PRACTICE

The language used in chatting is fragmented, associative and very colloquial; a chat participant must not only be fast but flexible enough to switch from one topic and even one discussion to another. The supporting role of the teacher is very important when assuring quality of content and balanced participation by all those who contribute to the chat. The younger students are, the more important it is that the chat is hosted and moderated by the teacher.

- Follow the discussion actively during the whole chat session.
- Agree on the schedule of the session beforehand: everyone should be present at the same time.
- Follow rules of netiquette: be polite, kind and respectful as if you were face-to-face.
- Remember that a carelessly written message can hurt even if this was not your intention.
- A short message works best. Do not monopolise a real-time chat session by pasting chunks of pre-written text which the others are obliged to read and respond to.
- Chat style is close to a stream of consciousness style. Carefully read others' messages to understand what they are trying to say. This may involve filling in the blanks.
- Remember not to share your username and password. Keep all of your private information private during chats or IM. Screenshots can always be taken of your information (or comments) and shared with others.

FURTHER INFORMATION

- Some ideas for school teachers can be found at:
  < http://www.educationworld.com/a_tech/chat-room-get-new-life-in-classrooms.shtml >.
- tChat is a chatroom in French: < http://www.tchat-orange.fr/index.php>.
- Information on "In-room chat as a social tool" can be found at:
  <http://www.openp2p.com/lpt/a/3071>.
- See Wikipedia for a list of basic emoticons:
  <https://en.wikipedia.org/wiki/Emoticon#Basic_examples>.
- Pew Research Center has studied mobile messaging and social media: <http://web.archive.org/web/20160703022409/http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/>.
- "What is snapchat and why do kids love it and parents fear it?": <http://web.archive.org/web/20160619055301/http://www.forbes.com/sites/larrymagid/2013/05/01/what-is-snapchat-and-why-do-kids-love-it-and-parents-fear-it/#65fc2b447875>.
- In Denmark, Cyberhus is using "group chat" as a valuable platform for helping enhance the well-being of vulnerable teens and foster their increased participation in society:
  <http://cfdp.dk/2015-cyberhus-chat-counselling-last-year/>.

---

17. http://www.netlingo.com/word/real-time-chat.php
18. https://en.wikipedia.org/wiki/Internet_forum

Social networking and social sharing

Asocial network service or social networking site (SNS)[1] is a platform used to create social networks among people who share similar interests or activities. This web-based system provides a variety of means for users to interact, such as chat, messaging, e-mail, video, voice chat, file sharing, blogging, discussion groups and so on.

▬ Social networks are based around personal profiles containing key personal data, interests, network of friends and similar. Social networking sites bring together communities of people who share interests and activities, or who are interested in exploring the interests and activities of others. They provide different types of software[2] for users to do this.

▬ Social networking sites allow people to connect with each other (usually with self-description pages for each network member) and provide recommender systems built on trust to link users. Some sites contain directories of specific categories of users (such as former classmates).

▬ Social sharing allows users to share content from a website on a social media site or application[3].

1. https://en.wikipedia.org/wiki/Social_networking_service
2. https://en.wikipedia.org/wiki/Social_software
3. www.oxforddictionaries.com/definition/english/social-sharing

■ Popular global social networking sites and apps include: Twitter, Facebook, LinkedIn, Google+, Snapchat, Tumblr, Pinterest, Vine and Whatsapp.

■ European-based sites and apps include: Badoo, Bebo, Vkontakte or VK (Russia), Delphi, Draugiem.lv (Latvia), iWiW (Hungary), Nasza-Klasa (Poland), Soup (Austria), Glocals in Switzerland, Skyrock, The Sphere, StudiVZ(Germany), Tagged, Tuenti (mostly in Spain) and many more.

■ Social networks are equally important for exchanges on human rights and fundamental freedoms and can provide relevant information to the wider public.

■ Most social networks are organised around life experiences but there are also other communities:

- communities of transactions, which facilitate buying and selling, renting properties or rooms, etc.;
- communities of interest which are commonly centred on a specific topic, such as movies, health, etc.;
- communities of fantasy which are based around imaginary environments and game-playing such as "World of warcraft" and "Second life";
- communities of human rights and/or activism on issues affecting the users;
- communities of support and advice related to disabilities, special needs or other challenges.
- Most social networks also offer simple features for managing the privacy of personal data (see Fact sheet 9 on privacy settings). These tools allow users to restrict access to parts of their profile to only their friends, or only members with certain credentials. They also allow members to restrict access by random searches and the availability of their content to tagging by other members.

IMPORTANCE IN EDUCATION

- Social networking and social sharing are inexpensive and rapid ways of sharing content, from personal information to marketing information.
- Social networking allows people to stay in touch as well as reconnect with family and friends that they may have lost contact with or who are living at a distance.
- Networking sites also allow for the organisation of events. Some events can be innocent, ranging from a jewellery show to a children's party, while others can cause harm, such as a rave party or demonstration for a racist/xenophobic/homophobic or other extreme and disparaging cause.
- Many industries are seeing the importance of social networking and branding, and aim to get referrals (and eventual sales) via social networking.
- Because of the ease of social sharing via websites and apps on smartphones, many young people are sharing anything and everything without much scrutiny.
- Responsible social networking is crucial, as potential employers, colleges or universities, or even family and friends, can obtain access to that information.
- Responsible social networking can be seen as an inexpensive way for self-promotion, (for example a young person starting a campaign for a community service), creating viral content for the benefit of social good, or even for recognition (when a young person posts information about an award or certificate recently earned).
- Social networking sites can be used to promote information that is false or based on biased views, requiring extra diligence on the part of users in choosing "friends" and checking to see that content is reliable.

ETHICAL CONSIDERATIONS AND RISKS

■ People often talk of losing their inhibitions when using social networking sites. They feel empowered and sometimes invincible, making comments and saying things to others that they would not normally consider in a face-to-face conversation. This is further exacerbated by the fact

that it is very easy to exaggerate emotions in the virtual world or to say things you would keep private if you were communicating face to face with someone.

▬ Social networking sites allow users to leave comments on other peoples' profiles. Consideration needs to be given as to the type and nature of such comments.

▬ As cited by UK's Get Safe Online[4], some of the risks of using social networking sites include:

- disclosure of private information by either yourself or friends/contacts;

- bullying;

- cyber-stalking;

- access to age-inappropriate content;

- online grooming and child abuse;

- encountering comments that are violent, sexual, extremist or racist in nature, or offensive activities and hateful attitudes;

- people trying to persuade or harass you into changing your basic beliefs or ideologies, or to adopt an extremist stance;

- prosecution or recrimination from posting offensive or inappropriate comments;

- phishing e-mails allegedly from social networking sites, but actually encouraging you to visit fraudulent or inappropriate websites;

- friends', other people's and companies' posts encouraging you to link to fraudulent or inappropriate websites;

- people hacking into or hijacking your account or page;

- viruses or spyware contained within message attachments or photographs;

- you or a family member posting that you are away or going away on holiday and therefore advertising that your home is empty, leaving the way open for burglars; if you do so and you make an insurance claim for a burglary while you are away, your insurance company may well reject it for this reason[5].

▬ But there are also other risks such as:

- exposure to commercial content and exploitation of your private data for commercial purposes;

- permanent damage to your online reputation, which may lead to difficulties in finding employment or various other discriminations such as financial exclusion (inability to get a loan or an insurance, etc.);

- being exposed to one-sided content in line with your own beliefs/knowledge/opinions which may limit personal growth and evolution;

- being subject to extreme social pressure to look perfect, have an interesting and happy life and continuously post impressive/cool things.

▬ As with all online technologies, banning young people from using technology is not the answer. Young people need to be empowered to behave safely and discriminately when online, and encouraged to respect age restrictions, keep their personal information private and be responsible publishers.

▬ Responsible adults should educate themselves about the dangers and good practices for safe usage of social networking sites, rather than trying to stop them from being used. All of these things will be done naturally in the offline world – so why not in the online world too?

---

4. https://www.getsafeonline.org/social-networking/social-networking-sites/
5. www.getsafeonline.org/social-networking/social-networking-sites/

▬▬ Young people need to be encouraged to talk about their online experiences with trusted adults such as parents and teachers. As with all other Internet safety issues, the single biggest positive impact on young people's online behaviour results from an active engagement by parents and teachers in their online life.

▬▬ This has a positive effect on adults too, since they learn about the positive features of social networking sites.

IDEAS FOR CLASSROOM WORK

- Ask students to consider the sort of information that they think it is acceptable to publish to an online profile. Once they have come up with a list, ask them to create a profile on paper. Would they be happy for this profile to be sent home to all parents at the school? In most cases, students would not want this to happen but they should be reminded that anyone can look at their profile on a social networking site unless it is set to private. Making this link between the real world and the virtual world is important as it helps children and young people realise the implications of posting online.

- Look at two or three social networking sites in class and get students to highlight any risky behaviour they can see. Discuss what it is that is putting the users at risk. Now ask your students to review their own online activities in the light of the points they have just picked up.

- Have your students work in groups to create their own checklists of points to watch when they are publishing material online on a social networking site. Compare lists and combine them to make a single class checklist that students can print out and take home to post on the wall next to their computer.

- Have your students bring in digital photos that they would like to upload to a social networking site. Working in small groups, analyse each photo to see what private information is being disclosed. Give a "safety rating" to each photo on a scale of 1-5, attributing 5 to any photo that perfectly safeguards the user's privacy.

- See section on Web 2.0 , 3.0 and more (Fact sheet 3) for further suggestions about how to use these social networking technologies within the classroom.

- Prepare suitable material for your children or students to open a discussion on what extremist content is, and how it can impact on behaviour. Work with them to come up with ideas on how to counteract extremism. The Council of Europe action plan against violent extremism and radicalisation will be useful to inform students and trigger ideas[6].

- Look at the General Data Protection Regulation with your students and discuss why the European Union may wish to limit access to social networking for children below a certain age[7]. What age should this be?

GOOD PRACTICE

- Anyone can access the personal information you post – the rule of thumb is to assume that everything is public unless you make sure that it is not. Consequently you should not say anything on a social networking site which you would not be willing to broadcast in public in the offline world. Opting for the private profile setting does not always mean that only friends can see a profile. In some cases it means that everything put on a profile can still be seen by everyone, but only "friends" can post comments or IM (instant messaging). Also you should be aware that if you join big groups or networks (e.g. country or city networks), this may give huge numbers of people access to your profile.

6. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3576
7. http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_citizens_rights_2016_en.pdf

- Trust your instincts – if it does not look or "feel right", it probably is not! If you find something online that you do not like or that makes you feel uncomfortable, turn off the computer and talk to a trusted friend about it.

- Be careful with personal information. The problem is that as soon as a person posts personal information to the Internet, he/she has lost control over who will see it and how it will be used. Pictures can easily be copied and shared with thousands of others at the press of a button. Because of the digital nature of the photos, they can even be altered or distorted. They can also be used by new search software to identify people even if the picture is not attached to a name. We all need to learn to only post pictures we would be happy for everyone to see, including parents and teachers.

- Not everyone online is who they appear to be. The fact that certain websites claim to connect students from the same school means nothing. The information provided by users when they are registering is not checked. Anyone can create a user profile pretending to be someone else. Moreover, anyone can join as many school communities as they want, regardless of their real or pretended age.

- Keep it balanced – if social media has become an obsession and you cannot live without checking/updating your profile, posting pictures and counting "likes", then you may want to take some "social media time-off", or at least keep a check on the time you spend on social networking sites.

- Review the materials provided by most social networking providers on guidance within their sites for safe use.

- Consider carefully the material that you post online – remember that once you post some-thing you may never be able to completely delete it from the Internet.

- Be especially careful in posting images. Even if you do not put your name next to an image, it can still identify you and can remain available in web caches long after you take it down.

- Protect your personal information, especially information that could identify or locate you.

- Never post anything which may be offensive, defamatory or degrading to others.

- Remember that your profile can be set to public or private. You should consider carefully which is the most appropriate setting to use.

- Make use of the privacy features offered by social networking sites. Think carefully before opening your profile to public viewing.

- Remember that if your profile setting is public, it can be seen by anyone. Even if it is not public, it may be seen by everyone in the networks you are a member of. It is a good idea to verify your settings from time to time, as social networking sites may change their policies.

- If you experience problems such as hate campaigns, bullying or targeted messages with racist, xenophobic, homophobic or other extreme content always ask for help from someone you trust, even if you think they might not understand or approve.

- Never give away your contact details on your profile.

- Remember that the contents that you post online may be used for a number of purposes including personalised advertising and even for employability or political reasons.

- Check your settings when you access social networking sites from different devices as they may ask permission to access your information from your smartphone, tablet or computer.

FURTHER INFORMATION

- For more on social networks, see "The world's 21 most important social media sites and apps in 2015": *<http://web.archive.org/web/20160423200413/http://www.socialmediatoday.com/social-networks/2015-04-13/worlds-21-most-important-social-media-sites-and-apps-2015>*.

- For advice on "Safe social networking", see: *<http://web.archive.org/web/20120602054510/http://www.getsafeonline.org/nqcontent.cfm?a_id=1459>*.

- Information on a variety of topics related to using social networking sites and tips on staying safe can be found at: *<www.privacyrights.org/social-networking-privacy>*.

- There is a Social Science Research Network report on teens' use of social networks at: *<http://web.archive.org/web/20160703112245/http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128>*.

- PEW Research Center has published a review on teens, technology and friendship on: *<http://web.archive.org/web/20160710143035/http://www.pewinternet.org/2015/08/06/teens-technology-and-friendships/>*.

- Relevant Council of Europe documents: Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services: *<https://wcd.coe.int/ViewDoc.jsp?id=1929453>*.

Privacy and privacy settings

Privacy refers to the degree of control that a person has concerning access to and use of his/her personal information. Most e-mail and Internet users assume that personal information will not be used without permission and that information exchanges are private and secure. The reality, however, is very different.

▬ Every time you access a website, post content on social media or send an e-mail, you leave information about yourself that could include your physical and computer address, telephone and credit card numbers, consumer pattern data and much more.

▬ You should also remember that once your data is out there, you may have difficulty retaining control over it and there may be long-term consequences.

▬ As e-commerce – including online shopping and advertising – becomes a frequently accepted way of doing business, special consideration should be paid to the protection of sensitive data, communications and preferences.

▬ There should be no lasting or permanently accessible record of the content created by children

on the Internet if it poses challenges to their dignity, security and privacy or renders them vulnerable now or at a later stage in their lives (Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet, adopted on 20 February 2008)[1].

▬ Privacy is closely related to security; be sure to read thoroughly Fact sheet 19 on security.

INTERNET PRIVACY

- Internet (or online) privacy is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications and preferences[2].

- Internet privacy is a concern every time a user goes online via computer, tablet, smartphone, gaming console or other Wi-Fi enabled device.

- Internet privacy does not just refer to how you keep your data private online, but also to the accessibility for hackers to retrieve your information.

- The General Data Protection Regulation provides users with more control over their data and affords them more online privacy. The key considerations for the GDPR include:

  ► a new definition of user consent – consent can no longer be considered as having been given freely if users have to consent to the processing of more data than is strictly necessary for the provision of that service;

  ► better transparency in informing users about how their data is being processed with the use of pictograms/icons and "plain language" – this will allow users to better compare services and choose those with a higher respect for privacy;

  ► users' right to data portability, meaning they will be able to retrieve their data in a usable format from the services they use – user control over their data and the principle of data ownership is greatly enhanced with this provision;

  ► enhanced protection for children – any child between the age of 13 (minimum) and 16 (maximum) will benefit from extra protection, such as requiring parental authorisation for processing data and protection against data processing for advertising purposes;

  ► stronger fees (up to 4% of a company's turnover) in the case of a breach of these rules.

- If a password is hacked, compromised and revealed, the consequences could be very serious, ranging from identity theft to illegal online transactions and more.

Privacy settings

▬ Privacy settings are the controls that allow users to limit who can access your information and how much information can be seen by others.

▬ Privacy settings on most social networks are initially set to a default position; you can usually customise these to your own requirement and should re-check them every time the social network platform advises you that it has implemented upgrades.

▬ Privacy settings should be verified regularly and on all Wi-Fi enabled devices. Remember to check geolocalistion settings too, as the location co-ordinates of you/your device are important aspects of your privacy (see Fact sheet 5 on mobile technology).

Geolocalisation

▬ Geolocation[3] is the identification of the location of an object, such as radar, mobile phone or Internet-connected computer.

▬ Geolocalisation is the process of identifying the location of an object. Geolocation apps report

---

1. https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2820.02.2008%29&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75
2. http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy
3. https://en.wikipedia.org/wiki/Geolocation

your location to users and they can also identify the distance to real-world locations in comparison to your location. Geolocation apps have opened up new business models for services and products.

▬ Geolocation can be a threat to your privacy as it pinpoints where you are and the geolocation of a child can also pose a threat to that child's security.

Cookies

▬ A cookie[4] is a text file left on your computer when you visit a website. It cannot harm your computer, but will give access to information about your behaviour and interests. This can provide a more personal surfing atmosphere. For example, when registering with a website, you may be greeted by name upon your return.

▬ It is important to decide how private you want to keep your online behaviour. Since cookies can be used to track usage patterns and contact information, they provide a possibility for encroachment on your privacy. They also facilitate behavioural targeting from advertisers[5].

▬ You can use anti-spyware[6] to help control the data your system is broadcasting and to clean out unwanted cookies.

▬ Today, all websites owned in the EU or targeted towards EU citizens are expected to comply with the Cookie Law (EU Directive 2009/136/EC). This gives individuals the right to refuse the use of cookies that reduce their online privacy.

Data protection

▬ The protection of personal data is regulated by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

▬ You have the right to know what data a business has about you. You should also be able to modify it if it is not accurate and you need to give your consent on how this data is being used.

▬ The best guidelines for protecting your data can be found in the General Data Protection Regulation[7].

▬ Read the disclaimer carefully on all websites and apps where you are asked to provide private information[8]. This is a legal agreement between you and the data controller[9] and should provide details on where and how long your data is stored, and how to have it deleted.

▬ Make sure your machine and e-mail programs are password-protected[10]. When you get a new device or software, or sign up with an Internet service provider, a "default" user and password setting will probably be provided[11]. Make sure you rapidly change such default settings to a more secure password and ID.

▬ It is best to encrypt[12] any sensitive information which is sent over the Internet. Fortunately this is standard for most e-commerce[13] transactions but you should still make sure that a page is secure before transmitting credit card information or bank account numbers.

▬ Different sections of your computer can be secured using passwords. Create passwords for folders containing valuable documents such as confidential projects, research, original designs and so forth.

Right to be forgotten

▬ The right to be forgotten is an important element in any discussion about privacy, as this right allows individuals to "retake" their privacy.

4. https://en.wikipedia.org/wiki/HTTP_cookie
5. https://en.wikipedia.org/wiki/Behavioral_targeting
6. https://en.wikipedia.org/wiki/Spyware
7. http://ec.europe.eu/justice/data-protection/reform/index_en.htm
8. https://en.wikipedia.org/wiki/Disclaimer
9. https://goo.gl/XEkvjh
10. https://en.wikipedia.org/wiki/Password
11. http://www.netlingo.com/right.cfm?term=default
12. http://en.wikipedia.org/wiki/Encryption
13. http://en.wikipedia.org/wiki/Ecommerce

▬▬ In the European Union, a person can ask a search engine to erase certain results from its index that will not come out when someone looks for his or her name. But there are limits and this measure will always need to be balanced against other people's fundamental rights, such as freedom of expression. In any case, the information will still be accessible in the website where it is located; this will only make it more difficult to find.

▬▬ To exercise the right to be forgotten and request removal from a search engine, one must complete a form through the search engine's website[14].

▬▬ But remember, it is better not to post private information in the first place because once it is on Internet it is almost impossible to completely delete.

Importance of talking about privacy in class or at home

▬▬ The technical and social aspects of privacy and the risks of self-disclosure provide valuable learning themes. Technical aspects may be included in information technology (IT) studies, but should equally form part of a life-skills curriculum.

▬▬ An important element of education on privacy should be the concept of "profiling" and the linking together of scattered elements of information about a person to deduce a more detailed picture. The important educational implication is that a lot more information can be found about us by "putting two and two together". For example, an "anonymous" social networking profile (hiding behind a pseudonym) may be identified with your real-name by matching photos between the anonymous profile and a full profile on another site.

▬▬ The idea that privacy is only violated by the disclosure of classic personal information should be examined carefully. New marketing techniques, which discriminate between people based on their behavioural traits (namely, behavioural targeting), may also be considered to be privacy invasive.

▬▬ Privacy is being increasingly undermined by the rapidity and ease with which children and young people can publish and/or stream digital images on the Internet through web applications and via camera and MMS facilities on mobile phones. A simple rule of thumb: never publish anything you do not want your teachers or parents to see.

▬▬ Everyone should have the skills necessary to navigate the Internet safely, and that includes knowledge of self-protection, effective communication and responsibility towards others.

▬▬ There is a natural flow from this theme into the citizenship dimension of any curriculum. The issues raised about online privacy accurately mirror social issues predominant in most cultures today. Exploring the motivations of hackers[15], crackers and privacy activists offers rich possibilities to discuss the value of democratic principles.

ETHICAL CONSIDERATIONS AND RISKS

- Online privacy is one of the most complex ethical and legal topics regarding the Internet.

- Everyone has a right to privacy and needs to be protected from malicious intent.

- Internet privacy risks include phishing (Internet hacking to steal secure user data); pharming (Internet hacking to redirect a legitimate website visitor to a different IP address); spyware (offline application that obtains data without a user's consent); and malware (an application used to illegally damage online and offline users through Trojans, viruses and spyware)[16].

- Sexting, that is the act of sending suggestive and explicit content, images (often selfies) messages, videos, via phone, computer, webcam or other device or writing sexy posts online has serious consequences not only in legal terms but also with respect to reputational risks for the person involved, as messages, images or videos may be posted on social media sites or used in pornographic websites and videos.

---

14. https://en.wikipedia.org/wiki/Right_to_be_forgotten
15. http://en.wikipedia.org/wiki/Hacker
16. http://web.archive.org/web/20160703014430/https://www.techopedia.com/definition/24954/internet-privacy

- We are accountable for all decisions we make about our own and others' rights, for example copyright[17] and intellectual property[18].

- Freedom of speech is a right; however, in practice this is a grey area with no easy answers. What is acceptable and what is not? How does one enforce the rules without encroaching on the rights of the speaker?

HOW TO

▬ Using privacy settings on all of your Wi-Fi enabled equipment with Internet access is one of the best ways to protect your privacy.

▬ Depending on your browser, do a quick search on privacy settings to see how you can:

- block ads and tracking
- block third party cookies
- block websites from accessing your location.

▬ Do not forget to set privacy settings on smartphones, tablets and gaming consoles. The latest cameras have geolocation settings you should check too.

IDEAS FOR CLASSROOM WORK

- Have students do a Google search on their own names. Be sure to look under images and videos as well. Have them create a Google alert on their own names so that they will know when their name has been posted online.

- Create a basic knowledge framework for privacy with your class. Define concepts, both technical and social, and identify prejudices and myths for discussion. Simply setting the questions "What is privacy?" and "Is privacy necessary?" should generate some strong views.

- Search for privacy sites on the Internet and use traceroute[19] programs to locate the physical addresses of these sites to demonstrate the diverse geophysical issues governing legality on the Internet. Explore other issues (cultural, political and historical) that come up from the trace results. For example, choose a remailer[20] site or anonymous proxy service, run a trace, then search for reasons why the services would be located in those countries.

- The Play-Decide role play game on data protection and privacy[21] offers a fun way to explore the implications of privacy law, copyright and freedom of speech, and information across national boundaries or for different age and cultural groups.

- Teach students how to create secure passwords[22].

- Explore and compare user profiles on some of the more popular social networking sites with your students (see Fact sheet 8 on social networking). What private information are users inadvertently disclosing? Draw up a checklist for creating a safe user profile.

GOOD PRACTICE

- Two golden rules:
  - ▶ do not share your personal information with anyone you do not know and trust;
  - ▶ do not use another person's personal information or photo without their consent.

---

17. http://en.wikipedia.org/wiki/Copyright
18. http://en.wikipedia.org/wiki/Intellectual_property
19. http://en.wikipedia.org/wiki/Traceroute
20. http://en.wikipedia.org/wiki/Remailer
21. http://paneuyouth.eu/files/2013/06/PD-kit-privacy-and-data-protection.pdf
22. http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password

- Back up[23] your system, and have a regular backup policy.

- Update security measures on your system and do some research on additional tools at *<http://www.epic.org/privacy/tools.html>* that will support your online preferences.

- Anti-virus[24] and firewall[25] software are an absolute necessity. You might also want to consider other tools such as pop-up blockers[26] and anti-spyware[27]. Be sure to check your system regularly.

- Use "strong passwords"[28] to protect your PC, e-mail and Internet connections. Strong passwords consist of letters, numerals and special characters.

- Before giving out private data, check for the locked padlock symbol that shows up in the toolbar. This is a sign that your transaction is taking place over a secure connection. Before making online transactions, check that the URL includes HTTPS; the S stands for "secure" in the Hypertext Transfer Protocol (HTTP) and authenticates the website and the associated web server, which protects against third-party attacks.

- Avoid online shopping on unreliable websites and avoid exposing personal data on websites with lower security levels.

- Be sure to check your rights; you may be more protected than you think. Users are always the weakest link in privacy and data protection.
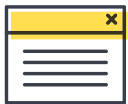
FURTHER INFORMATION

- To read more about the Cookie Law and the EU Directive, see: *<http://www.cookielaw.org/the-cookie-law/>*.

- There is a European Commission Fact sheet on the right to be forgotten: *<http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>*.

- There is also a European Commission Fact sheet on data protection *<http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf>* and other information on related reforms *<http://ec.europe.eu/justice/data-protection/reform/index_en.htm>*.

- The Electronic Privacy Information Center (EPIC) maintains a list of privacy tools and articles: *<http://www.epic.org/privacy/tools.html>*.

- Find out what your PC is telling anyone on the net who cares to look by using BrowserSpy: *<http://gemal.dk/browserspy/>*.

- Concerned about your civil liberties? These discussions on privacy could keep your citizenship class going for a while: Electronic Frontier Foundation at *<http://www.eff.org/>*, Epic.org at *< http://www.epic.org>*, Privacy International at *<http://www.privacyinternational.org/>* and Privacy.net at *<http://www.privacy.net/>*.

- TuCows at *<http://www.tucows.com/>*, is a website which provides access to over 40 000 shareware and freeware programs. It promises fast, local and safe virus and spyware-free downloads.

- Zone Alarm at *<http://www.zonelabs.com/store/content/home.jsp>* is one of the better known firewall programs. It lets you set access controls for different programs which send information out over the Internet.

- CryptoHeaven is an encryption package which offers secure mail, file sharing and chat with symmetrical and asymmetrical encryption: *<http://www.cryptoheaven.com/>*.

---

23. http://en.wikipedia.org/wiki/Back_up
24. http://en.wikipedia.org/wiki/Antivirus
25. http://en.wikipedia.org/wiki/Firewall_%28networking%29
26. http://en.wikipedia.org/wiki/Pop_up#Add-on_programs_that_block_pop-up_ads
27. http://en.wikipedia.org/wiki/Spyware
28. http://en.wikipedia.org/wiki/Password#Factors_in_the_security_of_an_individual_password

- Facebook Help Center provides information on privacy settings: *<https://www.facebook.com/help/193677450678703>*.

- Statistics on how children and young people understand online privacy and privacy settings can be found on *<http://web.archive.org/web/20160703155259/https://www.techopedia.com/2/30101/internet/online-privacy/do-millenials-understand-online-privacy>*.

- For statistics on being young in Europe today, see *<http://web.archive.org/web/20160604111543/http://ec.europa.eu/eurostat/statistics-explained/index.php/Being_young_in_Europe_today_-_digital_world>*.

- For information on European digital rights, see *<http://www.edri.org>*.

- Relevant Council of Europe documents:

  ▶ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108): *<http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>*.

  ▶ Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet: *<https://wcd.coe.int/ViewDoc.jsp?id=1252427>*.

  ▶ The Council of Europe page contains information about the work of the Council of Europe in the field of of privacy and data protection: *<http://www.coe.int/en/web/internet-users-rights/privacy-and-data-protection>* as well as information about your rights and responsibilities online.

3. Internet – Participating in the knowledge society

> " "Knowledge is power. Information is liberating. Education is the premise of progress, in every society, in every family."
>
> *Kofi Annan, former Secretary General of the United Nations, January 1997-December 2006*

CHECKLIST FACT SHEET 10 – SEARCHING FOR INFORMATION

Do you read the disclaimer when you are consulting a website?

How can you be sure the information you find is factual and objective?

Do you consult several websites to check your facts?

CHECKLIST FACT SHEET 11 – FINDING QUALITY INFORMATION ON THE WEB

Before downloading files, do you check that your anti-virus software is active?

If you get your news from the Internet, do you seek multiple perspectives on the same story?

Clean out your cookies from time to time to avoid being "profiled" by search engines.

CHECKLIST FACT SHEET 12 – DISTANCE LEARNING AND MOOCs

Choose a method of distance learning that is appropriate for you: determine what type of learning (synchronous, asynchronous, open schedule, hybrid distance learning) will best help you reach your goals.

Before selecting a distance learning course, research the reviews – both from students and teachers.

Take adequate precautions to ensure that your computer equipment and software is secure from hackers, viruses and other threats.

CHECKLIST FACT SHEET 13 – SHOPPING ONLINE

Do not make online purchases on unsecure Internet connections.

Understand and agree to the key information provided about the product or service.

Disable in-app purchases on your smartphone or tablet.

Do not believe all user recommendations you see, creating "user" recommendations can also be a money-making business.

Searching for information

At the very start of the Internet, there were no search engines. Try to imagine a world without search engines. People had to find websites printed on paper, or in magazines and type the address into their browser. Hopefully, that website had links to another website and by clicking from one link to another, they could "explore" the World Wide Web. Progressively, Internet portals or directories[1] were created, which were a bit like a phone book: a vast list of websites sorted into categories. Some of these directories or portals still exist, such as Yahoo! and MSN.

━━ Other forms of portals include:

• portals with "official" content such as the United Nations website or the Council of Europe website;

• portals specialised in specific content or services such as Booking.com for hotels or Amazon.com for shopping;

---

1. https://en.wikipedia.org/wiki/Web_portal

- portals that are based on user generated content, which are very diverse – social networks such as Facebook can be considered as a form of portal too.

▬▬ Search engines were then created and they revolutionised the way people searched for content on the Internet. But how do search engines work? Today, search engines rely on web crawlers[2] and very sophisticated algorithms that analyse content, classify content in indexes[3] and decide which websites to pull from those indexes depending on the keywords you use in your search.

▬▬ The way the algorithm is set up is extremely important as most people stop at the first few pages of search results. Google is the most popular search engine today and it made itself popular thanks to its algorithm which used an original method of ranking a website's importance, based on how many backlinks[4] it has. This basically means how many external websites include links to your website. For instance, if the wikipedia.org website is referenced on a large number of other websites, then it gets ranked higher.

▬▬ But algorithms get tweaked constantly for increased accuracy. For instance, Google plans on adding an element that calculates the "trustworthiness" of websites based on cross-referencing the content with facts stored in Google's Knowledge Vault. Moreover, algorithms can also be tweaked for commercial purposes, as we will see later.

▬▬ Check out Google's animated explanation on how their search engine works: *<https://www.google.com/insidesearch/howsearchworks/thestory/>*.

EDUCATIONAL VALUE, WHY IS IT RELEVANT, IMPORTANT?

▬▬ Learning how to use a search engine properly is arguably the most important skill one should develop not only to surf the Internet responsibly, but also to acquire transversal skills such as critical thinking (by searching for and comparing divergent sources online). Once you understand how to use a search engine, it can help you find quality information to develop a thousand other skills or gain increased knowledge about an infinite array of topics including – behaving responsibly on the Internet!

▬▬ For instance, you can build up your digital skills by searching for solutions to problems you experience with your devices or simply satisfying your curiosity about how they work. Finding this Internet literacy handbook, the very one you are reading now, can happen thanks to using a search engine.

ETHICAL CONSIDERATIONS AND RISKS

- Some portals may require membership or registration, which may be a paid service. Before you register (even for "free" services) make sure that you understand the terms and conditions of service, and that you have examined and understood the privacy policy of the website (see *<http://www.netlingo.com/right.cfm?term=privacy%20policy>*).

- Websites use a variety of means, including payment, to improve their ranking in search engine results. Some search engines, such as Google, clearly identify which results are sponsored advertisements. Many others do not make this distinction.

- The algorithms themselves are never neutral and are subject to controversy and criticism[5]. For instance, Google was known to increase the visibility of its own services such as Google Shopping, Google+ or YouTube at the detriment of its competitors (Amazon, Facebook, Dailymotion, etc.). Search engines can also be manipulated for political reasons. As a rule of thumb, never believe that, just because a search result is ranked higher, it is representative of the "truth" or that lower ranked websites are "unimportant" or "irrelevant".

---

2. https://en.wikipedia.org/wiki/Web_crawler
3. https://en.wikipedia.org/wiki/Web_indexing
4. https://en.wikipedia.org/wiki/Backlink
5. https://en.wikipedia.org/wiki/Criticism_of_Google

- This is why it is essential to have several gateways and search engines capable of searching the Web in order to get more diversified results and maintain a healthy competition that can contribute to better search accuracy and neutrality. As a user, you play an important role in shaping the online environment: do not forget to use other search engines such as Yahoo!, Bing, Qwant, IXquick or DuckDuckGo. By using less known search engines, you contribute to their continued existence and thereby secure diversity[6].

- Be aware that your geo-location[7] and cookies from your previous searches will influence your search results. Although your geo-location data being picked up by the search engine is unavoidable[8], periodically deleting your cookies (see Fact sheet 9 about privacy and privacy protection) and – to a lesser degree – your browsing history, will reduce the targeted ads you receive related to your latest searches (e.g. travel destination). It will also help ensure that you are reasonably well informed on important social and political issues by not limiting you to your perceived perspective[9]. You can also disable cookies altogether by looking at your settings inside your Internet browser; however, beware that some websites might not function properly.

- Finally, keep in mind that the results you get to your searches will depend greatly on what you search for. For instance, if you search for very violent content, that is what you are likely to find, but you may get much more than you ever wished for. Developing resilience to shocking or disturbing content is a lifelong process, so do not get ahead of yourself, take it one step at a time.

HOW TO

Because search engines are the most important gateways in accessing information, it is essential to understand how they work in depth. Sticking to the search results of the first page could give you an extremely truncated vision of what is important and what is not. The most important advanced search features to remember are:

- Quotation marks: this is probably one of the most useful and most well-known advanced search features. If you want to make sure that a search engine looks for an exact expression, use quotation marks around it. This may be useful if you want to find an exact phrase or expression.

- Minus sign "-": this is for when you search for something but exclude a specific term. For instance, if you search for "twilight", the first results will be all about the movie series. But if you search for "twilight -vampire", you get the definition of the word "twilight". The minus sign is therefore very useful when a word is too often associated with something else and you want to make sure that it does not get mixed up in your search.

- Query options: you can add a specific option to your search by using certain key words. For instance, if you type "define: bird", it will search for the definition of "bird" instead of searching for the word in general. If you type "site: wikipedia.org apple", Google will only search the "Wikipedia" website. This is very useful when searching through portals as we will see below. There are many more query options, so go check them out in the link provided below.

- Specialised searches: most search engines, including IXquick, Qwant, DuckDuckGo, Google, Yahoo! and Bing, have specialised search options, such as searching for multimedia content (images, videos, etc.), academic papers, books, maps, and so forth. Get familiar with these specialised search possibilities, as they come with their own advanced options. For instance, you can filter images by size, colour, file type and even copyright and licence.

- Search tools: the "search tools" available directly below the search bar once you have made a search, are also extremely useful. You can filter results by country and by time. This is very useful if you search for news for instance, as you can restrict the search to the most recent news or news published exactly one year ago.

6. https://en.wikipedia.org/wiki/Web_search_engine
7. http://www.advancedwebranking.com/blog/geo-location/
8. http://www.allaboutcookies.org/cookies/cookie-profiling.html
9. http://www.pcadvisor.co.uk/how-to/internet/how-delete-cookies-web-browsing-history-3218163/

- Advanced search: the "advanced search" option can be found by clicking on the upper right "options" button. Advanced search provides you with all of the above search features in a user-friendly way so, if you are not comfortable using the operators or specific query option terms, use "advanced search"[10].

IDEAS FOR CLASSROOM WORK

- Set a search target for any topic: create teams that use different portals/search engines, as well as a team that uses some of the search techniques described above for searching for information. Allow the teams to compare results, ease of access and quality of information.

- Create a topic for exploration, for example 18th-century art depicting children, or ecosystem dynamics of a particular species in the ocean. Provide your class with portal URLs[11] that will lead to links supporting the lesson plan. As there will probably be too many links for individuals to follow, create teams to divide up the links and cover as many as possible, allowing each team to present their findings. Team results may differ, thus providing a narrower focus for further refinement of the students' learning.

- Prevention or cure: get students to look up their own name on a search engine and see how much unwanted information they find about themselves. How can they prevent such information being available to all and how can data protection regulations help them have unwanted content deleted?

GOOD PRACTICE

- Maintain a healthy skepticism about material you find. The Internet offers a free space for people to share opinions and put forward ideas. Be sure to evaluate with a critical eye and search for divergent opinions and information in order to avoid propagating myths or falling for false claims.

- Avoid falling into plagiarism by using ready-made essays or work. As far as possible, credit the author and give the source of material you quote or use. This is important because:
  ► it gives the author and source due credit;
  ► it protects you from accusations of plagiarism;
  ► it helps others form their own judgment about the credibility of the material;
  ► be conscious of copyright issues if you use material you find on the Internet (see below the "How to" section and Fact sheet 14 on music and images).

- Take the time to manage/clear your cookies and your browsing history. You can disable cookies altogether for enhanced privacy, but bear in mind that some websites may not function properly without them.

- Always try several search terms, advanced search techniques and various search engines to get the most out of your search and find a diversity of sources for your query.

- Bookmark useful sites or portals so you do not have to search for them again.

- Sometimes, you will be looking for something related to a portal, such as an official document from your public administration, the definition of a word, comparing hotel prices or air fares, or buying a product. For all of these queries, you can use a combination of search engines and well-known portals such as Booking.com, Wikipedia or Amazon. Many portals have their own internal search engines, but you can also use an external search engine and restrict the search to that portal. For instance, search for "Hotel Brussels site: booking.com". Trying both is good practice to find what you are looking for.

---

10. https://www.google.com/advanced_search?hl=en; https://en.wikipedia.org/wiki/Google_Search#Search_options
11. http://en.wikipedia.org/wiki/URL

- If you find useful material, print, take a screenshot or save it. You may not find it again or it may be taken offline without warning.

- If you cannot find the answers through a search engine, post a query in a relevant message board, discussion forum or social network.

- Do not forget to contribute to content creation online. All the answers that you are looking for when using a search engine have been typed up and created by someone. Sharing your own knowledge and skills might help someone else someday (see Fact sheet 15 on creativity).
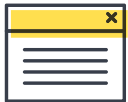
FURTHER INFORMATION

- Wikipedia is a free-content encyclopedia, written collaboratively by users from around the world: *<http://www.wikipedia.org/>*.

- The Europeana portal hosts vast amounts of digitised content representing the cultural heritage of Europe: *<http://www.europeana.eu/portal/>*.

- These European search engines have high standards for privacy protection: *<https://www.qwant.com/>* and *<https://ixquick.com/>*.

- There is also a US search engine with high standards for privacy protection: *<https://duckduckgo.com/>*.

- The following site tells you how to search on the Google search engine: *<https://support.google.com/websearch/answer/134479?hl=en>*.

- For tips on using Bing on Microsoft on Windows 8, see: *<http://onlinehelp.microsoft.com/en-us/bing/jj684589.aspx>*.

- How do search engines work? See: *<http://web.archive.org/web/20160509142554/http://www.bbc.co.uk/guides/ztbjq6f>*.

- Relevant UN Convention on the Rights of the Child articles:

  Article 13 – Children have the right to get and to share information as long as the information is not damaging to them or to others.

  Article 16 – Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

  Article 17 – Children have the right to reliable information from the mass media. Television, radio and newspapers should provide information that children can understand, and should not promote materials that could harm children.

- Relevant Council of Europe documents:

  ▶ Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines: *<https://wcd.coe.int/ViewDoc.jsp?id=1929429&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>*.

  ▶ Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters: *<https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282008%296&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>*.

Finding quality information on the Web

The original idea behind the creation of the Internet[1] was to develop an electronic library for the easy access and distribution of information[2]. In many ways this goal has been accomplished: today the Internet functions as an enormous library where most public and private libraries from across the world are present. They provide information about services, programmes and activities, and give access to physical books listed in catalogues and which can be ordered over the Internet. Digital libraries give access to books and collections online, usually digitised as html script[3] which gives the appearance of a web page[4], as Word or PDF documents[5] or as plain text (ASCII)[6]. Some major libraries and museums enable you to browse through their digitised versions of rare books and artefact collections[7].

1. http://www.livinginternet.com/i/ii_summary.htm
2. http://www.livinginternet.com/i/ii_summary.htm
3. https://en.wikipedia.org/wiki/HTML
4. http://en.wikipedia.org/wiki/Html
5. http://www.census.gov/main/www/pdf.html
6. http://en.wikipedia.org/wiki/ASCII
7. http://www.bl.uk/manuscripts/Default.aspx

▭▭ The Internet also goes way beyond libraries in offering information and can provide up-to-date, reliable information on whatever interests you: current affairs, technologies, hobbies, entertainment, art, sports and more. This is available through a broad range of sources including 24-hour news channels[8], newspapers[9], journals[10] and news aggregators, commonly known as newsfeeds or RSS feeds (rich site summary, see *<www.whatisrss.com>*), and these are available through many websites and social media platforms. Users subscribe to these to regularly receive the latest aggregated web content from online newspapers, blogs, podcasts and video blogs (vlogs) in one location for easy viewing.

▭▭ Today, around many Europeans keep up with national and international news via the Internet, and use it to obtain health information. Getting news from social media platforms is also a growing trend. News discussion forums and newsgroups offer fertile platforms for discussion and a means of getting multiple perspectives on topical issues whilst also sharpening students' debating skills. There are hundreds of thousands of such forums worldwide and the more active groups receive hundreds of new messages each day. The messages are divided into threads, which record and display the sender's name and the time the message was sent. Most servers and browsers today can point you to forums of interest to your students[11].

▭▭ Twitter is another means of getting information updates from the Internet. You can use your own Twitter address to follow news outlets, journalists and experts in the fields you are interested in, or sign up to a Twitter list so that you can follow anonymously[12]. Google alerts can similarly be used to follow news on specific topics, but if the key terms are not carefully and clearly defined you may receive too many alerts to be useful. Social media platforms are progressively adding new functions to keep you updated on world news too.

IMPORTANCE IN EDUCATION

- The research skills necessary to navigate both traditional and online libraries are similar. It is crucial that children are guided by their parents and teachers to learn and practise these skills from their first steps on the Internet.

- There are thousands of category-specific libraries on the Web at *<http://vlib.org/>* and *<http://www.sldirectory.com/libsf/resf/libplans.html>* that relate specifically to curriculum areas and themes. "Essentially, webquests are mini-projects in which a large percentage of the input and material is supplied by the Internet. Webquests can be teacher-made or learner-made, depending on the learning activity the teacher decides on."[13] The model at *<http://webquest.org/>* can be very useful when creating activities for classroom participants to use library facilities on the Internet while developing a range of core skills, such as research, archiving, literacy, analysis and evaluation.

- Newsgroups and discussion forums are a useful resource for developing critical thinking and debating skills, on condition that young people are encouraged to check their facts by consulting several different sources. They can also provide a platform to share information and learn from the experience of others.

ETHICAL CONSIDERATIONS AND RISKS

- Cookies (the small files left on your online device to store information about you and your preferences) can improve your browsing experience by remembering your preferences or avoiding that you sign in each time you visit certain sites. However, by using cookies, search engines will lead you only to like-minded sites, and could gradually narrow your perspective on news stories and topical issues.

8. http://wwitv.com/news_tv_live/
9. http://www.onlinenewspapers.com
10. http://www.e-journals.org
11. http://www.newsforum.com
12. https://en.wikipedia.org/wiki/Twitter
13. https://www.teachingenglish.org.uk/article/webquests

- The Internet has democratised journalism by giving people of all ages the possibility to actively contribute content. The offer of information on the Internet is therefore becoming endless, underlining more than ever the importance of distinguishing between quality and unreliable content and also between information and infomercials, that is, advertising that looks like objective information.

- Very few newsgroups or discussion forums are fully moderated and users are not tracked. They can therefore be exploited for illegal activities, such as distribution of copyrighted material, racist propaganda, extremism or child sexual abuse material. Using such platforms requires a certain sense of responsibility and awareness of acceptable social conventions, as the supposed anonymity they provide can lead to anti-social behaviour, such as posting nasty messages, bullying and flaming[14]. Students should also be led to reflect on privacy issues when they use such forums[15].

- Most libraries will provide access according to certain rules. These rules[16] will require at least that the user honours the copyright criteria of the material. Remember that unless the materials are in the public domain, you may not redistribute or publish them without the permission of the publisher. Copyright is also a personal responsibility. Plagiarism is the use of someone else's work without crediting the source. Be sure to credit your sources, and instil the habit among your students.

HOW TO

- Usenet[17] is a worldwide distributed discussion system that consists of a set of "newsgroups" with names that are classified hierarchically by subject. Access to these newsgroups is defined by your Internet service provider (ISP) or school, university or business server[18]. Access to some platforms is free, whilst "premium" services work on a subscription basis.

- Many tools exist for setting up a news or RSS feed. The video "Get organized: streamline your news feeds"[19] provides a step-by-step description of how to use the tools that best suit your needs.

- To set up Google alerts, you first need to create a Google account. You can then type in a list of words, set a few other parameters and Google alert will inform you via e-mail or feed when those terms appear online. You will receive a list of URLs showing updates on your term, or you can add the alert to an RSS feed reader of your choice.

- Using a current theme in your classroom, identify a category library at *<http://vlib.org/>*. Consider building a webquest around resources from this library, or use an existing webquest at *<http://webquest.org/>and<http://www.spiritsd.ca/teacherresources/default.asp>*. You can find webquests by using a search engine[20]. Enrich your webquest by setting up a Google alert or joining a Twitter list[21], and compare the quality of information you receive from each.

- Adults, children and young people can find quality news websites and activities on the Scottish-based International Federation of Library Associations and Institutions (IFLA)[22] multi-language site. It offers a broad range of topics from art and history to science and maths. Others are available on the "Great websites for kids"[23] site, developed by a division of the American Library Association. Further information on library and information services can also be found on the IFLA site, which is considered to be the global voice of the library and information profession.

---

14. http://en.wikipedia.org/wiki/Flaming
15. http://www.webwewant.eu/information
16. http://web.archive.org/web/20160102210205/http://www.gallowglass.org/jadwiga/SCA/libraries.html#Copyright__Plagiarism
17. http://en.wikipedia.org/wiki/Usenet
18. https://en.wikipedia.org/wiki/Server_(computing)
19. http://web.archive.org/web/20151231202307/http://www.pcmag.com/article2/0,2817,2458165,00.asp
20. http://en.wikipedia.org/wiki/Search_engine
21. https://media.twitter.com/best-practice/create-and-use-twitter-lists
22. http://www.ifla.org/activities-and-groups
23. http://gws.ala.org

GOOD PRACTICE

- Before encouraging students to use online libraries, make sure to review basic library skills and research strategies[24]. Also ensure they have a solid understanding of copyright protection.

- Make sure there is an anti-virus filter on any devices being used to download files. Before downloading files[25] to the school server, check with your school network administrator that there is adequate protection in place and sufficient space for storing files and archiving[26] them appropriately.

- When setting information-finding tasks for your class, it may be wisest to provide your own list of URLs[27] to be used. In this way you can be sure that the addresses work and that the content is suitable.

- Many files that you will download will be in Adobe PDF format to protect copyright. Make sure that you have downloaded and installed a recent version of the Acrobat Reader in order to ensure that students can open these files. This can be done from the Adobe Systems[28] site.

- The basic safety principles you apply when using the Internet should be applied when using online libraries. Check privacy statements, conditions of usage and scan files for viruses.

- When first joining a newsgroup be sure to check the frequently asked questions - FAQ[29] for guidelines. This will give you an idea of the netiquette of the newsgroup. Different news-groups have different rules.

- Keep your messages as short as possible but make sure you give all relevant information. For example, if seeking the answer to a technical problem, give precise details about the hardware and software you are using.

FURTHER INFORMATION

- Google newsgroups at *<http://groups.google.com/>* has a complete list of newsgroups and an archive of over 1 billion postings.

- David Lawrence and Russ Allbery give advice on creating a Big 8 newsgroup: *<http://web.archive.org/web/20140330141231/http://www.faqs.org/faqs/usenet/creat-ing-newsgroups/part1/>*.

- Wikipedia has an entry for newsgroups: *<http://en.wikipedia.org/wiki/Newsgroups>*.

- The British Library offers digitised collections: *<http://www.bl.uk/manuscripts/Default.aspx>*.

- The World e-book Foundation offers thousands of texts: *<http://www.netlibrary.net/>*.

- The Library Spot provides a free virtual library resource centre: *<http://www.libraryspot.com/>*.

- "Teacher tap" has a list of 1 000 + webquests and related resources: *<http://eduscapes.com/tap/topic4.htm>*.

- In the teen publication the Web we want, the chapter "Information is not knowledge" *<http://www.webwewant.eu/web/guest/information>* provides interactive activities for teens to sharpen their critical thinking and journalistic skills.

---

24. https://www.pinterest.com/explore/library-skills/
25. http://www.walthowe.com/glossary/d.html#download
26. http://en.wikipedia.org/wiki/Archiving#Computing_sense
27. http://en.wikipedia.org/wiki/URL
28. http://www.adobe.com/products/acrobat/readstep2.html
29. http://en.wikipedia.org/wiki/Faq

Distance learning and MOOCs

Distance learning is a formalised teaching system where students and teachers are not physically present in a classroom together. The educational process takes place via electronic media; as technology has advanced, so has distance learning. We now see virtual classrooms where students and teachers exchange content via e-mail, instant messaging, video-conferencing, chatrooms, bulletin boards and more.

▬ Regardless of the technology used, distance learning remains a proven method that opens up lifelong learning opportunities to students of all countries and all ages, making it possible for them to earn diplomas, certificates and degrees from almost any online university in the world. Students are also able to have discussions with other students – or teacher(s) – who may be located hundreds or even thousands of kilometres away, which definitely adds an enriching element to learning.

▬ Distance learning began in the mid-1800s with generations of adults seeking advanced education at home, in the military or on the job. Courses used to be done by correspondence, with material sent back and forth through the traditional postal system. These days, however, distance learning

has evolved to take advantage of current technology. It thrives via the Internet, and students can study for degrees without ever setting foot in a brick-and-mortar classroom.

▬▬ Distance learning exists in different forms today, ranging from the classic definition above, to massive open online courses (MOOCs), to peer-to-peer YouTube training and webinars, or to Periscope for virtual field trips. Although technology has progressed rapidly, the fundamentals of distance learning remain the same: providing education.

TYPES OF DISTANCE LEARNING

MOOCs

- MOOCs were first introduced in 2008 with the goal of delivering content via the Internet to anyone who wants to take a course with no limit on attendance. Interactive community forums were created to allow exchanges between students and teachers.

- By 2012, MOOCs were being sponsored by formal educational institutions and one could find universities such as Stanford University, Princeton University, the University of Michigan and the University of Pennsylvania aligned with Coursera, a for-profit educational technology company.

- Other successful MOOC programmes include Udacity, another Stanford University partner, and edX, a MOOC provider founded by the Massachusetts Institute of Technology and Harvard University.

- MOOCs are based on a teacher-student model, whereas the existence of YouTube has created another type of distance learning model: peer-to-peer.

Peer-to-peer training

- Peer-to-peer training can be described as sessions where people learn from colleagues with similar backgrounds to theirs. An example could be children educating children, lawyers educating lawyers, etc.

- This co-teaching module is easily found on YouTube, where YouTube "teachers" with millions of subscribers offer software tutorials, website design tutorials, make-up tutorials, writing tutorials and thousands of other subjects.

Webinars

- Webinars or web-based seminars, can also be found across the Internet. Coaches, educators, gurus and anyone professing to share knowledge can offer a webinar.

- Webinar formats may include presentations, lectures, PowerPoint presentations, videos, work-shop materials and more.

- Webinars may also include downloadable materials to be worked on at a later date.

Periscope

- Periscope is a broadcasting app which allows people to see what you are seeing, in real time. The app has had unparalleled success in its first year and educators are still searching for useful applications.

- Some educators believe that virtual field trips, sharing their classrooms or getting real-time questions from student viewers might have uses; however, this is a distance-learning tool to monitor in the future.

▬▬ Advances in distance learning have revolutionised learning environments, from elementary school to tertiary education. For example:

- Lectures can be given via streaming media[1] or as printed material saved in files which are stored on the educator's server[2].

---

1. http://en.wikipedia.org/wiki/Streaming_media
2. http://en.wikipedia.org/wiki/Web_server

- Students communicate with the teacher and each other through message boards[3], e-mail[4] and chat[5].

- Open educational resources (OERs) are documents and media (usually open-licenced) that are useful for teaching, learning and assessing, as well as for research purposes. OERs provide yet another means of enabling teachers to use and exchange content with other schools, educators and continents. OERs are sometimes also created by non-teacher experts on specific topics, and can be easily shared and selected through a repository, such as OER Commons[6].

- Tools such as the above have given rise to the "flipped classroom", an instructional strategy and a type of blended learning that reverses the traditional educational arrangement by delivering instructional content, often online, outside of the classroom and moves activities, including those that may have traditionally been considered homework, into the classroom. Learn more about tools at Edutopia[7].

- Students can upload assignments into a drop box, which is a usually free-of-charge service, where registered users can keep files safe, sync them and easily share with whoever they choose. Even quizzes and exams can be automated and taken online.

- With MOOCs and distance learning, course materials are always readily available and can be easily updated. Moreover, these new learning environment formats provide unparalleled flexibility for self-paced work.

IMPORTANCE OF DISTANCE LEARNING

- The Internet is perfect for setting up a virtual learning environment. Students can, for example, stay in their own hometown while studying at a virtual university abroad or share their learning time across different places, for example between a company and a school for commercial students.

- Providing students with an access to the whole base of learning material gives them the opportunity to become more autonomous and gain a deeper understanding of why and what they are learning.

- Students have more ownership of their own learning, and the role of the teacher is transformed into the role of a coach.

- Courses are not restricted to the opening hours of "normal" schools or universities, so everyone can benefit from more opportunities to become lifelong learners.

- Distance learning changes the behaviour of both the teacher and the student. Successful students develop persistence and organisational skills and the teacher must become more conversant in technology.

ETHICAL CONSIDERATIONS AND RISKS

Accreditation

- The ability to distinguish between accredited and non-accredited programmes is useful when determining the legitimacy of the course provider.

- Accreditation badges for distance learning[8] are emerging in a wide range of areas and represent an important step in equity of learning opportunities.

- When programmes do not have actual accreditation but are partnered by well-known and established universities, they often carry some form of skill validation.

---

3. https://en.wikipedia.org/wiki/Internet_forum
4. https://en.wikipedia.org/wiki/Email
5. https://en.wikipedia.org/wiki/Online_chat
6. https://www.oercommons.org
7. http://www.edutopia.org/blog/flipped-learning-lets-talk-tech-jon-bergmann
8. https://wiki.mozilla.org/Badges

Teacher and faculty

- Distance learning does not change the fundamental requirement of having competent teachers. In fact, more than ever it underlines the need for teachers to be given more training opportunities to keep up with emerging educational trends.

- The value of face-to-face learning cannot be denied, but the benefits of technology and education are also noteworthy.

- Since anyone can set up their own webinar or peer-to-peer online course and even brand themselves as an "expert", critical thinking is as important for users here as it is with all other forms of web content.

HOW TO

You should be aware that you, as the user, are responsible for taking certain precautions when choosing a degree or other distance-learning programme. Here are some points to watch:

- Remember that there are dubious distance-learning institutions out there right alongside the legitimate ones. Make sure you research a programme/organisation thoroughly before enrolling;

- Security issues are always key, as with any exchange of information over the Internet. Viruses (see Fact sheet 19 on security) and hackers[9] can wreak havoc on a distance-learning system so be sure to consult Fact sheets 9 on privacy and 19 on security to see which precautions you should take;

- Copyright[10] is usually protected by the law of the student's home country. However, when following distance-learning programmes in other countries be sure to check that the learning sources are covered by international copyright.

IDEAS FOR CLASSROOM WORK

- Place students in groups of two, where one group is the "teacher" and the other is the "student". Have the students research a course topic and provide reasons why one type of distance learning would be better than another for that given topic.

- Once students agree on the distance-learning method and a course topic, have the "teacher" group research ideal course requirements and ask the "student" group to do the same. Compare and contrast the needs of teachers and students.

- Choose a method of distance learning and research and check what type of certification is available. Is it a reputable institution? What indicators tell you whether an institution is reputable? Does the institution offer certificates or badges?

- Discuss the difference between learning apps and learning courses. How can both provide new learning opportunities for people with disabilities?

- Invite students to set up their own short learning course on a topic in their favourite subject area and encourage other students to take the course. From this experience, have the class draw up a list of criteria that make online learning more effective.

GOOD PRACTICE

- The Internet is changing the way we learn and it is very important for students to have access to all information and tools available to help them learn.

---

9. https://en.wikipedia.org/wiki/Hacker_(computer_security)
10. http://en.wikipedia.org/wiki/Copyright

- The "digital divide"[11] is seen as a leading issue in the economic and social growth of many nations and the use of distance learning can narrow this gap. However, the opposing view notes that if there is a digital divide and people cannot access the Internet (and distance learning), then the gap will widen.

- Distance learning can increase student learning in measurable ways. It provides Internet training with hands-on experience for students, their families and teachers.

- Distance learning provides an opportunity for students to build new skills and qualifications and grow in new directions.

- Distance learning can also provide access to disabled students who may not previously have been able to attend a classroom. The students are able to participate in an online classroom and have exchanges with other students and the teacher.
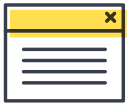
FURTHER INFORMATION

- The Distance Learning Portal provides information on distance learning programmes and institutions around the world: *<http://www.distancelearningportal.com/>*.

- The International Council for Open and Distance Education provides information and resources on international institutions: *<http://www.icde.org/>*.

- European Schoolnet, a consortium of European ministers of education, provides an OER repository for teachers: *<http://lreforschools.eun.org/web/guest>*. It also provides educational resources for special needs: *<http://lreforschools.eun.org/web/guest/sennet>*.

---

11. https://en.wikipedia.org/wiki/Digital_divide

Shopping online

E-commerce may be defined as the collection of services, software and procedures that allows the sale of products online. Almost anything can be bought online from books to holidays, from clothing to electronics. Apart from material goods, you can also pay for services such as access to online content.

■■■ E-commerce has undoubtedly brought positive benefits as shopping becomes easier and more convenient; however, e-commerce transactions are not without risks. And as the industry grows, so will the benefits and risks.

■■■ A recent trend shows that more and more children make online purchases (often via a parent's credit card account) before attaining the age of 18 or even holding a part-time job appropriate for a student. This has given rise to concern about children "virtualising" money and becoming unable to develop a sense of its value, which could have a major economic impact for their future.

IN-APP PURCHASES

- In-app purchasing refers to the ability of a smartphone or mobile device to facilitate the sale of products or services within a specific application or "app"[1].

- While in-app purchases bring profitability to businesses, they can be a problem for those who do not understand how in-app purchases work.

- In-app purchases have posed a particular problem for children and young consumers who may not be eligible to make purchases, but can with just a couple of clicks.

CONSUMER RIGHTS

- If you purchase a product or service online, you benefit from consumer protection rules including: delivery within the agreed time, being able to return unwanted goods and paying only for things that you have expressly agreed to purchase. For example, in the EU you have the right to return unwanted goods within 14 days of receiving them.

- If you purchase a product or service online, the trader must provide you with certain key information about the product or service, which is clear, correct and understandable, before you make the purchase.

- For a listing of the key information, consult the European Union websites noted below.

IMPORTANCE IN UNDERSTANDING THE ISSUES

Children and young people need to be well-informed consumers: they need to know whether they are eligible to make purchases online, what the terms and conditions for a purchase are and how to claim their rights in the event of a problem. As online shopping gains in importance, it is vital that children and young people understand how to become responsible consumers able to take advantage of the benefits and avoid the risks associated with shopping online.

- Uninformed shoppers, especially the young and elderly, may be vulnerable to online scams and online shopping fraud.

- Buyers and sellers in e-commerce generally do not know each other and this anonymity may desensitise people to knowing right from wrong.

ETHICAL CONSIDERATIONS AND RISKS

- Protect your credit card data, telephone numbers and other personally identifiable information. Hackers can obtain credit card information by accessing your computer or by breaking into insecure websites holding your information. Be wary of websites that ask to save your credit card information, as this information can be stolen.

- Avoid paying for items using a public Wi-Fi connection. With the ubiquity of hot spots located in coffee shops, hotels, airports and even public parks, hackers can tap into hot spots and capture your personal information.

- Criminals also obtain credit card or banking information by tricking people into giving them voluntarily. Phishing[2] falls into this category. These attacks often target users of online shopping or payment sites, asking them to "reconfirm" details.

- Since online shopping often involves payment by credit card, consumers need to manage their finances carefully to avoid overspending. Regularly review your credit card bill to make sure that you did not make an inadvertent purchase and that there are no unauthorised purchases.

1. http://www.techopedia.com/definition/27510/in-app-purchasing
2. http://en.wikipedia.org/wiki/Phishing

- Pay attention to "too good to be true" bargains. Go to the retailer's site to confirm whether the offer is valid.

- The Internet has seen a multiplication of payment methods: PayPal, Bitcoins, money transfer, mobile payments and others. Bear in mind that no payment method is completely safe so always practise caution when paying for anything online.

HOW TO

In order to shop online safely, consumers should remember that shopping online requires additional precautions.

- Make purchases only from reputable vendors. This may become difficult as more and more vendors enter the marketplace, but do your research.

- Make sure that your computer, tablet, or smartphone settings are set to optimal.

- Verify that the order checkout area is encrypted. Many sites use SSL (secure sockets layer) technology. Look for the padlock icon and a website address indicating that it is secure: "https" instead of "http".

- Save a copy of your order by either printing a copy or taking a screen shot. You will be able to use this as proof in the event of contestation.

- Check your statements often to ensure that you were not billed for a purchase that you did not make.

IDEAS FOR CLASSROOM WORK

- Educate students to find out about the retailer and the conditions of sale.

- Invite students, alone or in groups, to look on specific commercial websites for products or services, with a particular goal in mind. For example, planning a holiday according to a fixed budget (see Fact sheet 10 on searching for information).

- Plan an e-commerce website with your students (to sell school products, for instance) or do further work on existing initiatives of that kind already taken within the framework of the school. Study the structure of a good e-commerce website.

GOOD PRACTICE

- Find out about the retailer or vendor. eBay, for example, allows vendors to build a reputation according to their track record and feedback. Do not buy from untrustworthy sources, especially those advertised by spam (see Fact sheet 19).

- Make sure you are insured against fraudulent use of your credit cards. Check your statements carefully for any unauthorised purchases.

- Read the terms and conditions. The text may be long and technical but do not click to say you have read and understood it if you have not done so.

- Check for hidden costs. These may be taxes or delivery charges on the side of the seller. Customs duties may also be charged if you are ordering products from abroad.

- Is the site secure? A padlock or key symbol in the lower right-hand corner of the web browser will indicate secure pages. Look for SSL[3] certificates, which ensure that data is encrypted before it is sent.

---

3. http://en.wikipedia.org/wiki/Secure_Sockets_Layer

- Make sure that you have control of your personal data and refer to the General Data Protection Regulation for better understanding. Pay attention to boxes relating to the retailer's options to retain your data or contact you for marketing purposes.

- If you have any doubt about the seriousness of a website, do not hesitate to do some research online, and look for other consumer testimonials, reviews or experiences. Websites such as Trustpilot are usually a good indicator of the seriousness of a website and the customer experience[4].
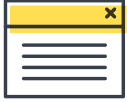
FURTHER INFORMATION

- Consult the European Union's website on online shopping: *<http://europa.eu/youreurope/citizens/shopping/buy-sell-online/rights-e-commerce/index_en.htm>*.

- Teach your students about online commerce, for instance from the Microsoft site: *<http://web.archive.org/web/20050405134258/http://www.microsoft.com/office/previous/frontpage/columns/edcolumn04.asp>*.

- The ECC-Net "promotes the understanding of EU consumers' rights and assists in resolving complaints about purchase made in another country of the network, when travelling or shopping online" *<http://ec.europa.eu/consumers/solving_consumer_disputes/non-judicial_redress/ecc-net/index_en.htm>*.

- TrustArc (formerly TRUSTe) is an independent, non-profit, global initiative aimed at building trust and confidence in online transactions: *< https://www.trustarc.com>*.

- The Europea.eu website offers information on online shopping: *<http://europa.eu/youreurope/citizens/consumers/shopping/index_en.htm>*.

- For information on the General Data Protection Regulation see: *<http://ec.europa.eu/justice/data-protection/index_en.htm>*.

- Paypal offers fraud prevention tips: *<https://www.paypal.com/eBay/cgi-bin/webscr?cmd=p/gen/fraud-tips-buyers-outside>*.

- For information on the OECD Recommendation on Consumer Protection in E-Commerce, adopted in 2016, see: *<https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf>*.

---

4. https://www.trustpilot.com/

4. Internet – For everyone

" "Creativity requires the courage to let go of certainties"

Erich Fromm, psychologist

CHECKLIST FACT SHEET 14 – VIDEOS, MUSIC AND IMAGES ON THE INTERNET

Check the licence of any content that you would like to reuse.

Use the Creative Commons classification on the content you create and post online.

Support fair online business models which enable you to pay for content from your favourite artist, musician or content creators.

CHECKLIST FACT SHEET 15 – CREATIVITY

One image can speak a thousand words, especially if we are not careful about our private information and that of others.

Do you understand how to ensure that your ownership of creative output is respected by others?

Plagiarism shows non-respect of creative ownership and can weigh heavily on multiple aspects of society. Are you aware of the multiple ways in which plagiarism can impact on society?

CHECKLIST FACT SHEET 16 – GAMES

Life balance is important: is the time you are spending online on games infringing on outdoor and face-to-face activities?

When the games you play online lead you to meet and communicate with strangers, remember that not everyone is who they say they are. Choose "human-moderated" games or games with "safe chat" through pre-selected phrases for very young children.

In-app purchases can be a trap for the unwary in certain games. Have you checked the tips in Fact sheet 13?

CHECKLIST FACT SHEET 17 – DIGITAL CITIZENSHIP

Do you know your online rights and responsibilities?

Have you checked your digital footprint lately? Put your name into a search engine and see what comes up.

What are the digital skills required to become a fully-fledged digital citizen?

CHECKLIST FACT SHEET 18 – DIGITAL PARENTING: POSITIVE AND PROACTIVE

Be positive when parenting in this new digital age and do your best to communicate with your child about what they are doing online, where they are going online and who they are talking to online.

Realise that even though technology has advanced in leaps and bounds, parenting remains much the same: staying active in your children's life, encouraging them to be good (digital) citizens and emphasising kindness and empathy.

Whether you are the parent of a toddler or a teen, be aware of the challenges of your child's development with respect to technology. Use technology in ways that help, not hinder, your child's development.

Videos, music and images on the Internet

The Internet, as a multimedia platform, offers a large number of modes of communication including exchange of audio files, video files and digital photographs. Applications and online platforms have largely facilitated the generation and dissemination of this kind of content, transcending linguistic, cultural and national barriers and raising important issues, related not only to the disclosure of personal information (see Fact sheet 9 on privacy) but also to copyright infringement and illegal or harmful content.

COPYRIGHT

- A number of international laws and agreements are in place. In 1996 more than 100 countries signed two World Intellectual Property Organization (WIPO) treaties, aiming to address digital content[1].

- A creator of audio-visual material automatically has copyright unless he or she waives it.

1. http://www.wipo.int/treaties/en/

- Most countries' laws maintain copyright for 50-70 years after the creator's death.

- There is usually more than one copyright holder of a piece of music. Author, performing artist, record company and publisher may all own rights or "related rights".

- Aside from the economic aspect, a creator of audio-visual content has "moral rights" [2]. This relates to the right to be recognised as the creator and the right for the work not to be altered or edited without permission.

- Music and films can be bought online (see Fact sheet 13 on online shopping). There are many sites for purchasing music online, for example iTunes[3] and Amazon[4]. But there are also many other online stores for buying music, images or videos, so feel free to make a search to find them.

- Buying music or films online usually gives limited or no right to copy or distribute them. For example, Apple's online music store iTunes allows a purchased track of music to be authorised on up to five computers within a household[5].

- As the consumption of multimedia content changes, new business models arise. Instead of buying a song, you can also pay a monthly subscription fee to an online streaming platform and listen to any song or watch any movie available on that platform. Examples of such services are Netflix [6] for movies and Spotify[7] for music. Again, many other platforms exist so feel free to do a search.

- The music industry has brought legal proceedings against both peer-to-peer software companies and individual file sharers. An uploader – someone who makes files available – is more likely to be prosecuted than a downloader.

- Creative Commons[8] is a non-profit organisation offering an alternative to full copyright.

⚠ ETHICAL CONSIDERATIONS AND RISKS

- At present, digital music sales account for 46% of the record industry's total sales with an increase of 6.9% in 2014. This is due to the multiplication of legal outlets for the sale or streaming of digital music (see *http://www.ifpi.org/facts-and-stats.php*).

- The music industry has also responded to piracy by filing a number of lawsuits against websites and individual users.

- Using peer-to-peer software[9] can be a security risk to your computer, as malware are often distributed by attaching them to music and image files.

- Consumption of multimedia content has considerably changed with the Internet. Instead of listening over and over to the same favourite CD, Internet users like to listen to a wide variety of songs and tunes, given the massive choice that the Internet offers. Each day, the average American listens to three and a half hours of music[10]. Ironically, piracy has contributed to forcing the industry to revise the "traditional" business model of purchasing a full album and opt for subscription based, unlimited streaming platforms. Remember that the decisions you make in choosing a streaming platform helps support its business model.

📖 EDUCATION

━━ Educational establishments are, in certain cases, allowed to reproduce works and communicate them to the public. Refer to your national legislation or to the European Union Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. The following conditions must be met:

---

2. https://en.wikipedia.org/wiki/Moral_rights
3. http://www.apple.com/itunes/
4. http://www.amazon.com/
5. http://www.apple.com/itunes/overview/
6. https://www.netflix.com
7. https://www.spotify.com
8. http://creativecommons.org/
9. https://en.wikipedia.org/wiki/Peer-to-peer
10. http://www.digitalstrategyconsulting.com/intelligence/2014/10/us_media_consumption_trends_music_tops_the_charts.php

► Works used must be solely for teaching or scientific research purposes.

► Source, including the author's name should be indicated – except where this is impossible.

► No direct or indirect economic or commercial advantage must be gained from the use of this content.

▬▬ Get written permission from a parent or guardian before publishing photos of children or young people online.

▬▬ In the case of content published on the school's website, all content, including content originating from children and young people, is under the authority and responsibility of the school.

IN THE CLASSROOM

- Have a discussion on moral aspects. Is piracy of audio-visual material stealing?

- Inform children and young people about the risks of viruses and spyware from downloads.

- Inform children and young people about the possibility of fines for downloading copyrighted music and film.

- Make children and young people produce an artistic/creative work in teams. This can be writing a poem, drawing a picture, writing a story, producing a video or composing a song. Ask them to look at the Creative Commons licence and choose the type of licence they want to apply to their content. When they are done, ask them to share their decision for the licence they chose and why: for instance, they chose to have a very restrictive licence because they intend to sell their creation or they chose to leave it open to modification and reuse and they fully understand that their work might be reused or transformed by someone else.

ILLEGAL CONTENT

- The definition of illegal content varies from country to country, but it most commonly refers to child pornography or child abuse material, extreme violence, political extremism, defamation or incitement to hatred against minority groups.

- Many countries have a hotline for reporting illegal content. INHOPE[11] is a network of national hotlines.

- Taking action against illegal content may be difficult or slow depending on the nature of the content and where it is hosted. Hotlines work together with Internet service providers (ISPs) and the police, and are best placed to tackle illegal content.

- Most online platforms use a variety of methods to identify and take down illegal content, for instance by using human and/or automated moderation, photo/video DNA technology and reporting mechanisms.

ETHICAL CONSIDERATIONS AND RISKS

- Illegal content is arguably a much more serious criminal offence than copyright. While there are notions such as "fair use" in copyright and exceptions for not-for-profit or educational purposes, illegal content will always be treated as a serious criminal offence, especially for cases such as child sexual abuse material or terrorism. While testing the limits to the various freedoms, such as the freedom of expression, is a natural trait of human beings, especially for children and young people, there are certain lines that should never be crossed.

- Illegal content is often linked with other illegal activities, such as selling illegal weapons or drugs. Much of this activity is taking place in the so-called "dark net", a part of the Internet

---

11. http://www.inhope.org/gns/home.aspx

which is not accessible via traditional search engines. Publishing, sharing or looking for illegal content might therefore easily snowball into very serious crimes.

- Your school or company should have an acceptable use policy (AUP), or alternatively a responsible use policy (RUP) that includes issues on copyright and illegal material.

- Whenever you find any content online that you would like to use, be sure to check the licence. There are many different licences. Content produced by regular Internet users comes with a variety of licences. The most "open" licence authorises you to reuse and modify the content without needing to notify the owner, even in commercial projects. Other licences ask for due credit to be given, limiting the use to not-for-profit, or forbidding any modifications. Search engines such as Google or Bing propose the filtering of image and video searches by licence. There are also many platforms where you can buy content to use inside your projects.

- Be sure to apply a copyright licence to your material. You can choose from a more traditional copyright, such as a record company, or use Creative Commons[12] classifications for material you create to clarify how others may use it.

- Although it may be tempting to look for music, images or videos for "free" online, remember that you always end up paying for it one way or another: by being subject to endless advertising, by infecting your computer with malware that may steal your data or even by getting a lawsuit from rights holders. Supporting platforms that provide good service and value for money contribute to shaping the Internet in a better way, avoiding filling it with time-wasting advertising, low quality or harmful content, and rewarding artists fairly for their work.

- Nowadays, content is being produced massively every day by users all over the world. Be it short videos posted on a video streaming platform, such as YouTube or Dailymotion, pictures and images posted on social networks, or music uploaded to music streaming platforms. But regardless of whether the user that uploaded it specified a licence or not, bear in mind that any content uploaded is protected. Only if the author has explicitly mentioned that he/she waives any rights on the content he/she has produced, does copyright law not apply.

- A further limit to the use of content is data protection. Re-posting an embarrassing video or picture, for instance, is a violation of someone else's data privacy and could be cyberbullying. As a general rule, always ask the user who originally posted content if you can reuse it, modify it, repost it or similar. Asking for permission and giving due credit is more than a legal obligation, it helps create a more positive and enticing environment for creativity and participation online. For more detailed information about data protection, visit the EU Justice site on the "Reform of EU data protection rules"[13].

GOOD PRACTICE

- Software filters can help block some illegal websites but are never a real solution. No filter can protect you if you proactively seek illegal content.

- As a parent, teacher or older sibling, be sure to trigger family and classroom discussions about online experiences. Illegal content is not just a matter of copyright, it is also often surrounded with harmful or shocking content, malware, spam and similar.

- Report illegal content to a hotline (see INHOPE below) or use the reporting mechanisms provided by the platform you use.

- Make sure that your school has a strict policy with regard to illegal content and that children and young people are properly informed about the potential consequences of publishing, sharing or viewing illegal content.

- Discuss harmful and illegal content. Surveys show many children and young people deliberately or accidentally find this type of content on the Internet, but few tell an adult.

12. http://creativecommons.org/
13. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

- Visit the World Intellectual Property Organisation (WIPO) website for more information on copyright and related issues: *<http://www.wipo.int>*.

- Learn what your favourite musical group has to say about musical piracy at "Artists speak out on music piracy": *<https://www.upvenue.com/article/1590-musician-stances-on-music-piracy.html>*.

- INHOPE is the network of hotlines for reporting illegal content on the Internet: *<http://www.inhope.org/gns/home.aspx>*.

- The Council of Europe media page has information on its work in the field of copyright: *<http://www.coe.int/media>*.

- The European Commission website offers information on intellectual property rights: *<http://europa.eu/youreurope/business/start-grow/intellectual-property-rights/index_en.htm>*.

- The IFPI, who represent the recording industry worldwide, offer a guide for parents and teachers to help explore music on Internet safely and legally: *<http://www.ifpi.org/music-and-the-internet-guide.php>*.

- The European Commission's Digital Agenda for Europe gives further advice on copyright: *<https://ec.europa.eu/digital-agenda/en/copyright>*.

- See the Wikipedia page for more information about the dark net: *<https://en.wikipedia.org/wiki/Darknet>*.

- Relevant UN Convention on the Rights of the Child articles:

   Article 13 – Children have the right to get and to share information as long as the information is not damaging to them or to others.

   Article 17 – Children have the right to reliable information from the mass media. Television, radio and newspapers should provide information that children can understand, and should not promote materials that could harm children.

   Article 33 – The government should provide ways of protecting children from dangerous drugs.

   Article 34 – The government should protect children from sexual abuse.

   Article 36 – Children should be protected from any activities that could harm their development.

   Article 37 – No one is allowed to punish children in a cruel or harmful way. Children who break the law should not be treated cruelly. They should not be put in prison with adults and should be able to keep in contact with their families.

   Article 40 – Children who are accused of breaking the law have the right to legal help and fair treatment in a justice system that respects their rights. Governments are required to set a minimum age below which children cannot be held criminally responsible and to provide minimum guarantees for the fairness and quick resolution of judicial or alternative proceedings.

Creativity

HOW DOES THE INTERNET PROMOTE CREATIVITY?

▬ Because of the flexible nature of the Internet, today's classroom setting is less rigid than ever before. Rapidly evolving technology gives students ample opportunity to explore topics that interest them and learn in non-traditional ways (see Fact sheet 3 on Web 2.0, 3.0 and more).

▬ Using the tools that modern technology provides, students can create professional-standard material that can be published for audiences anywhere in the world. They can produce their own online products and conduct experiments and simulations of all kinds within the classroom, or interactively with other learners across the Internet.

▬ The Internet has globalised education and provides the opportunity for students to reach out in real time to peers all over the globe. To fully exploit these opportunities, it is important that young Internet users become creators and not just consumers, an objective which underlies the many coding initiatives (for example, see *<http://codeweek.eu>*) being implemented in many countries today.

ENHANCING CREATIVE PROCESSES IN LEARNING

- Successful technology integration in the classroom offers students a chance to show their innovation, individuality and creativity, and to develop their entrepreneurship capacities.

- The use of creativity software and the Internet fosters motivation and improves learning in and beyond the classroom in meaningful ways. Coding helps develop a deeper understanding of how technology works, and can therefore contribute to more responsible user strategies.

- The possibility to express creativity and take on a more active role in the learning process encourages engagement and participation, two essential building blocks in citizenship.

- The Internet and mobile technology offer a multitude of exciting possibilities for teachers and students to create and upload their own audio-visual content. They can also use the Internet to contact artists anywhere in the world to ask for advice and opinions on their work. Artists can use video conferencing tools[1] and virtual meetings (see Fact sheet 12 on distance learning) to give workshops.

- Using social media[2] and dedicated social platforms[3] in classroom learning encourages students to work together, collaborating online on shared projects. This provides a new creative outlet, and the brainstorming involved can stimulate the creative process.

ETHICAL CONSIDERATIONS AND RISKS

- **Equity issues:** does everyone have the necessary equipment and connection to access the Internet? Are all children and young people the world over, regardless of age, ability or special needs, able to benefit from equal opportunities to be creative, that is to know how to use all available technology to be creative.

- **The online safety factor:** do the filters[4] put in place to protect young users, especially very young children and those with special educational needs, inhibit in any way access to the material needed to be creative? How can this be dealt with so that students can enjoy safe access to content they need (see Fact sheet 20 on labelling and filtering).

- **Training opportunities for teachers:** students can often be more Internet savvy than their teachers. Teachers need to benefit from more training opportunities in order to properly guide their students in all aspects of ICT, including mobile phone usage (see Fact sheet 5 on mobile technology, and Fact sheet 12 on distance learning).

- **Technical support issues:** adequate technical support in schools is necessary so that programmes and projects are not inhibited.

- **A buffered environment:** creativity allows expression of a person's feelings as an individual. Although ideally we should avoid imposing any constraints on a young person's creative processes, it is important to underline principles of tolerance, empathy and respect regarding outputs, especially in group brainstorming settings. A teacher or class delegate should be present to guide the work in a constructive manner.

- **Privacy:** Web 2.0 and 3.0 have largely facilitated the uploading of photos and images to the Internet. Students should be aware that a single image can speak a thousand words and could put at risk their private information and that of others.

- **Copyright:** young people need to learn from the earliest age to respect the ownership of creative output, and understand the cost of plagiarism to society[5]

1. http://web.archive.org/web/20080614214250/http://www.netlingo.com/right.cfm?term=video%20conferencing
2. http://www.eun.org/teaching/smile
3. http://www.etwinning.net
4. https://en.wikipedia.org/wiki/Content-control_software
5. https://www.teachingcopyright.org/handout/copyright-faq.html

BOOSTING CREATIVITY IN THE CLASSROOM

- A webquest[6] is an inquiry-based approach to integrating the Internet into the classroom.

- Students can challenge their creativity by learning the basics of coding[7] to build their own websites. This stimulates creative thought processes in different ways by requiring input on graphics and content.

- Students can collaborate on projects that develop writing and audio-visual production skills by producing online stories and other content. Mobile phones can be used, for example, to record and exchange images and video on cultural or occupational aspects of their own country with students from abroad. This can help them to learn through practice about concepts related to privacy, photo permissions and more.

- Encourage students to create interactive quizzes and activities for the Web with software such as Hot Potatoes[8] or interactive stories with multiple outcomes using software such as that available at Quia's[9] website.

- Secondary school and university students can create their own 3D learning environment with software like Active Worlds[10]. They can build their ideal landscape or their own virtual campus. They can also collaborate with other students in projects on different topics.

GOOD PRACTICE

- The Internet can be used as a basic research tool for background information on different topics. Students can then apply the knowledge they have gained in an assignment that stimulates creativity. Technology provides students with the opportunity and the freedom to develop higher-order thinking.

- The Internet and other modern technology allows for powerful communication and collaboration between students of different countries and cultures. More than ever before, students have the possibility to brainstorm creative solutions with a broad peer base.

- Open source software enables students from all over the world, especially children from less privileged households, to express their creativity for free. Software such as Open Office, Gimp, Audacity or Blender enables children to create documents, edit images or audio files, or even get into 3D animation at no cost. Furthermore, open source software offers the opportunity to learn about coding and sharing your skills by joining a community of motivated volunteer coders to enhance and update the software you use. Be sure to point out such alternatives to your children/students.

- Teachers have found that implementing technology in the classroom in such a way as to provide hands-on activities allows students opportunities for problem solving and innovation.

- Keep learning goals in mind: the key to reaching these goals is to focus on the process taken to get to the product rather than on the product itself.

- When students publish the results of creative activities online, they need to respect copyright[11] and perhaps learn more about Creative Commons[12]. Remind them to cite their sources when using material created by others.

---

6. http://webquest.org
7. https://scratch.mit.edu/educators/
8. http://hotpot.uvic.ca/
9. http://www.quia.com/
10. http://www.activeworlds.com/
11. https://en.wikipedia.org/wiki/Copyright
12. https://en.wikipedia.org/wiki/Creative_Commons

A number of websites can be used as a starting point to involve students in projects where creativity is encouraged and collaboration is essential:

- International Schools Cyberfair is an online meeting place where parents, students and educators can collaborate, interact, develop, publish and discover learning resources *<http://www.globalschoolnet.org/GSH/>*. European Schoolnet provides similar resources for schools: *<http://www.eun.org>*.

- The Future Problem Solving Program International engages students in creative problem solving by simulating critical and creative thinking skills: *<http://www.fpsp.org>*.

- Ideas and resources for promoting creativity can be found at Education Scotland: *<http://www.educationscotland.gov.uk/learningandteaching/approaches/creativity/>*.

- John Hopkins School of Education's New Horizons for Learning *<http://education.jhu.edu/PD/newhorizons/>* is a repertory of new didactical practices to promote creative learning.

- Chapter 6, "The artist in you", in the handbook Web We Want *<http://www.webwewant.eu>* provides a range of activities that lead young people to examine their own creativity and to learn more about plagiarism, copyright and much more.

Games

Video games can be described as entertainment that involves human interaction with a user interface to generate visual feedback on a video device such as a television screen, computer, tablet or smartphone. The term comprises a huge array of genres from arcade and role-playing to strategy games and fantasy worlds. eSports is the term for game competitions where participants (often semi-professional gamers) compete for money prizes in front of a rapidly growing live and online audience – this can be any sort of game, not just sports. Games can be played alone, with partners in closed circles or can involve thousands, or sometimes millions, of strangers playing together. Such massively multiplayer online games (MMOGs) include "World of warcraft" and "Game of thrones". Video games are now the third biggest sector in the entertainment market worldwide behind broadcast and cable television, generating sales of USD 74 billion as of 2015, after doubling income between 2013 and 2014[1].

---

1. https://en.wikipedia.org/wiki/Video_game

■ Smart phones and tablets and the presence of ever younger and older users on the Internet have had a considerable impact on gaming trends; 2015 research[2] shows that approximately 1 in 3 children under the age of 18 play online games but the average age of online gamers is 31 years. Previously more a male-dominated domain, today women account for 50% of all purchases, 48% of electronic game players worldwide and 52% in the UK. The use of dedicated game consoles has evolved too, with owners now spending more than half their time on consoles viewing television, streaming video, watching Blu-ray discs and exploring the Internet[3].

■ Games have forged a broader path as both a family and a classroom activity too. Of K-8 teachers, 74% say they include online games in classroom activities, with 4 out of 5 being "educational" games. Also, 56% of parents say that games positively affect their children. Given the increasing popularity of games and the impact they can have on human rights, the Council of Europe has published a set of guidelines for games providers, developed in collaboration with games providers and experts from child protection, education and human rights sectors[4].

■ This shows that online gaming is indeed big business, with a very broad variety of games being enjoyed by millions of users through the Internet and on mobile phones every day.

PERSONAL DEVELOPMENT AND EDUCATIONAL VALUE

- Game playing is more than entertainment; it is an enriching collaborative activity enjoyed by children and adults of all ages. It fosters creativity and interaction and plays an important role in social and intellectual development.

- Games represent one of the rare occasions when adults and children can exchange ideas on an equal footing (intergenerational communication).

- Children learn about democracy by playing within different social structures, in an environment bordered by rules and parameters.

- Games often involve sharing and respecting the rights and property of others, sometimes even bringing players into contact with other cultures and intercultural practices. Children can practise social skills without fear of failure and with a sense of control. Because games require children to obey rules and follow directions, they increase their capacity for self-discipline and autonomy.

- Puzzles, board games, adventures and quests offer opportunities for players to develop strategic thinking and problem-solving skills. Certain games can be used to increase fine motor and spatial skills in younger children and for therapeutic purposes with the physically disabled.

- Some studies imply that game playing can be useful in autism, and games such as Minecraft have been especially noted.

- Online games are useful for introducing newcomers to technology and coding, and generally fostering interest in and understanding of ICT[5].

- Games can be integrated into almost any area of the curriculum, from mathematics to social studies and languages.

2. http://web.archive.org/web/20160420163852/http://www.bigfishgames.com/blog/2015-global-video-game-stats-whos-playing-what-and-why/
3. http://web.archive.org/web/20151023082205/http://www.nielsen.com/us/en/insights/news/2015/game-consoles-in-2015-one-stop-shop-for-games-and-entertainment.html
4. http://www.coe.int/en/web/portal/guidelines-for-providers
5. https://en.wikipedia.org/wiki/Information_technology

ETHICAL CONSIDERATIONS AND RISKS

- Links between video games and addiction, aggression, violence, poor social development, and a variety of stereotyping and sexual morality issues have been under debate for several decades, with no conclusive evidence yet that these aspects in games are any more influential than through other media[6].

- Age appropriateness of games is important, even more so for very young children.

- Addiction is often cited as a risk. The American Psychiatric Association (APA) concluded in 2013 that there is insufficient evidence to include game addiction as an official mental disorder, but proposed the term "Internet gaming disorder" and urged for further studies to define criteria for this. While Internet gaming disorder is proposed as a disorder, it is still debated how much this disorder is caused by the gaming activity itself, or whether it is to some extent an effect of other disorders[7].

- Life balance is an important aspect when looking at gaming, as with all activities on the Internet. Time spent on gaming should not infringe on outdoor and face-to-face activities.

- Some online games allow the possibility to meet and communicate with strangers. Ensure that games encouraging user interaction, especially those intended for very young children, are supervised through human moderation or provide a "safe chat" with pre-selected phrases.

- Through in-app purchases, there is the potential in some games for children to inadvertently spend a large amount of their parents' money on collectibles and tools.

GOOD PRACTICE

- Labelling and rating systems encourage games industry actors to act responsibly by requiring them to define and describe their products. This also helps game buyers judge the content and age suitability of games, and to navigate the game market more safely. PEGI (Pan European Game Information) is the only pan-European classification system that provides detailed recommendations regarding age suitability of game content. The ratings of approximately 20 000 games can be found on its website <*www.pegi.info*>. PEGI is also part of IARC (International Age Rating Coalition), which provides a global rating and age classification system for digitally delivered games and apps[8] . As a result, PEGI ratings are now also available for all products in the Google Play Store and the Mozilla Firefox Marketplace. Microsoft Windows Mobile and Windows 10 app stores will follow very soon.

- Monitor the number of hours spent playing. Take action if other social activities are avoided or children and young people skip school in order to spend time gaming.

- Gaming communities can foster a sense of belonging and can lead children to trust too readily. Remind them that online friends may not always be who they say they are. It is important not to give out personal information to anyone online.

- Online gaming is becoming a popular family activity and provides a valuable opener to family conversations about responsible Internet usage. If parents or teachers are concerned that their children are spending too much of their time on electronic games, check out the many "gaming addiction tests" you can find through a search engine – these are also ideal conversation openers.

- The Council of Europe has produced an attractive, interactive online game[9] with the aim of promoting children's rights and protecting them from violence of any form.

6. https://en.wikipedia.org/wiki/Video_game_controversies#Crime_and_violence
7. https://en.wikipedia.org/wiki/Video_game_addiction
8. http://www.globalratings.com
9. http://www.wildwebwoods.org

- Choose a role-playing game for your class or family on a topical issue at *<http://www.playdecide.eu>*. You can also create your own game following the Play-Decide model and share it with others by uploading it to this website.

- In-game purchases, that is new content, game functionality, features and/or upgrades for a particular game or app, but also sometimes separate items in online stores outside of a game, are a growing area of concern especially to parents. Parental control filters can often prevent this.

FURTHER INFORMATION

- Look at "Ask about games" *<http://www.askaboutgames.com/>* to help make sense of video games.

- Read about ongoing game studies in the International Journal of Computer Game Research: *<http://www.gamestudies.org/>*.

- Legislation on video games is a vast subject that can involve criminal, regulatory, constitutional, administrative, company, contract and, in some jurisdictions, competition law. The public policy section of the ISFE (Interactive Software Federation of Europe – *<http://www.isfe.eu/objectives/public-policy>*) provides useful insight into relevant EU and global legislation.

- The Pan European Games Information (PEGI) website contains rating and labelling information: *<http://www.pegi.info/pegi/index>*. PEGI Online, an addendum to this system, aims to ensure a safer online gaming environment. Game providers licenced with a PEGI Online label meet the PEGI Online Safety Code *<www.pegionline.eu>* standards which include, amongst other things, obligations to try to keep websites free of illegal and offensive user-created content and undesirable links, to protect privacy and which have an independent complaints mechanism.

- Age verification is challenging in the games industry, as in other online sectors that appeal to young children. Pilot projects are underway in Europe to see if it would be possible to set up an "attribute exchange" whereby companies that sell or provide access to age-restricted goods and services could pool and exchange information to make age verification more effective.

- News stories are published every week about online games, as this is the fastest growing entertainment market. Consult several sites to get a balanced view of top-selling games, games news, descriptions, research reports and statistics. Useful starting points are Bigfishgames, IFSE, PEGI and Nielsen websites. You could also subscribe to the newsfeeds/newsletter these sites offer or set up a clearly defined Google alert to stay informed.

Digital citizenship

The widespread use of the Internet and new communication technologies has been a powerful engine for growth and jobs and has improved the quality of life for many citizens. Daily use of the Internet has become a common occurrence for many; however, a deeper understanding of digital citizenship and digital rights may be lacking.

The informed participation of all citizens in what is known as the digital environment depends on the development of a much broader literacy. This includes the ability to critically analyse the variety of information we are subject to (that is, audio-visual content), to form autonomous opinions, to be actively involved in community issues and to master new forms of social interaction. In a publication two decades ago already, UNESCO described these capabilities as the four pillars of education: learning to know, to do, to be and to live together[1]. Moreover, being a digital citizen requires being able to use web tools (see Fact sheet 3 on Web 2.0, Web 3.0 and more) and understanding the issues of e-privacy (see Fact sheet 9).

---

1. http://www.unesco.org/education/pdf/15_62.pdf

WHAT IS DIGITAL CITIZENSHIP?

- Digital citizenship is a term that describes how a person should act[2] while using digital technology online[3].

- Some experts propose nine elements that comprise digital citizenship: digital access, digital consumerism, digital communication, digital literacy, digital etiquette, digital law, digital rights and responsibilities, digital health and wellness, and digital security[4].

- Whatever the composition of digital citizenship may be, it is clear that all users of the Internet have a responsibility and possibly even a duty to act responsibly when using the Internet and communications technologies.

Digital footprint

- A digital footprint is the data that is left behind by users on digital services.

- A passive digital footprint is created when data is collected without the owner knowing, whereas active digital footprints are created when personal data is released deliberately by a user for the purpose of sharing information about oneself by means of websites or social media[5].

Digital identity

- A digital identity is information used to represent persons, organisations or machines in information systems and networks[6].

Digital literacy

- Digital literacy is the knowledge, skills and behaviours used in a broad range of digital devices such as smartphones, tablets, laptops and desktop PCs[7].

- Information and communication technologies have already reached into every aspect of our everyday lives, changing the type of skills necessary to be active members of society.

- As the Internet continues to evolve with the growth of wireless networks[8], increasing importance will be placed on people's ability to use today's technology to receive and transmit information efficiently in a way that transcends both media literacy and Internet literacy.

Digital rights

- The Council of Europe has produced a guide to "Human rights for Internet users" that explains digital rights and responsibilities in a user-friendly format, and underlines that human rights apply equally online and offline[9].

- The term "digital rights"[10] describes the human rights[11] that allow individuals to access, use, create and publish digital media or to access and use computers and other electronic devices or communications networks.

- The term is particularly related to the protection and realisation of existing rights, such as the right to privacy[12] , in the context of new digital technologies and, more especially, the Internet[13] .

- With respect to the digital rights of young people in Europe, the EU Youth Manifesto is an online "declaration" by European youth on how to make the Internet better[14].

---

2. https://en.wikipedia.org/wiki/Digital_citizen
3. https://en.wikipedia.org/wiki/Digital_electronics; https://en.wikipedia.org/wiki/Etiquette_in_technology#Online_etiquette
4. http://www.digitalcitizenship.net/Nine_Elements.html
5. https://en.wikipedia.org/wiki/Digital_footprint
6. https://en.wikipedia.org/wiki/Digital_identity
7. https://en.wikipedia.org/wiki/Digital_literacy
8. https://en.wikipedia.org/wiki/Wireless_network; http://en.wikipedia.org/wiki/3G
9. https://www.coe.int/en/web/internet-users-rights/guide
10. https://en.wikipedia.org/wiki/Digital_rights
11. https://en.wikipedia.org/wiki/Human_rights
12. https://en.wikipedia.org/wiki/Right_to_privacy or freedom of expression https://en.wikipedia.org/wiki/Freedom_of_speech
13. https://en.wikipedia.org/wiki/Internet
14. http://www.youthmanifesto.eu/

Digital citizenship and e-democracy

- E-democracy comprises the use of electronic communication technologies, such as the Internet, in enhancing democratic processes within a democratic republic or representative democracy. This is a political development being enhanced by the use of social networks which allow users to have their own voice and comment "in public" on relevant issues. One theory is that the use of social networks in e-democracy could enable broader influence on policy outcomes, as more individuals involved could yield smarter policies and increasing transparency and accountability.

- Nowadays politicians in many countries use social networking sites to engage with young people and seek their views. This is challenged by some, but it is important to go to the places where young people are in order to reach them.

- One concern about e-democracy is the impact of the digital divide on those who are not able to access the media. However, as a rapidly increasing number of people of all ages are accessing the Internet, this alone should not be seen as a consideration for not recognising the benefits of social networking sites in e-democracy.

- In offline communication, power is often seen as hierarchical whereas online this becomes diffused and constantly shifts. Similarly, online boundaries become permeable, roles are flexible, changeable and do not rely on non-verbal characteristics or hierarchy. These reasons alone illustrate the benefits of using social networking sites to promote e-democracy.

- However, for e-democracy to have a positive effect, users must be open to non-violent communication and contradictory views, and be willing to take part in pacific and respectful debate. When communities of like-minded people form and discuss issues without considering other perspectives, this can weaken rather than strengthen e-democracy and even lead to the radicalisation of opinions.

IMPORTANT IN EDUCATION

- The Internet makes it possible not only to publish far more information more rapidly but also to continually update this information so that citizens are informed of the latest developments in their areas of interest.

- The right to information and the right to participation are rights afforded to all children under Articles 13 and 17 of the United Nations Convention on the Rights of the Child.

- In the past, we had to rely on the versions of statements and events the press chose to publish to keep us informed; nowadays, we can very often go directly to the source to obtain our information first hand.

- As citizens around the world become daily journalists with their video-enabled smartphones, we are often inundated with "live" scenes unfolding before our eyes. The ability to scrutinise what the video presents and what happened before and after the filming commenced are often missing in such daily journalism, evidenced by Twitter feeds, YouTube videos, Vine streams and other social media platforms.

- The fact that citizens are better informed empowers them to better participate in the democratic life of their own country and on a pan-European and international scale. And citizens are able to use the Internet to research unbiased details concerning most issues.

- Geographical, traffic, cultural and tourist information collected by public and private sector bodies considerably enriches the lives of citizens. In some countries, citizens can even use the Internet to officially change their address, apply for passport renewal or carry out various other formerly time-consuming activities. Do not forget, however, that a certain number of precautions should be taken when giving out private information online (see Fact sheets 9 on privacy and 19 on security).

- The Internet also enables citizens to participate in online discussions and debates about topics of interest in public or local life, and even take part in elections by e-voting[15].

- In addition to political involvement, citizens can shop online, study online (see Fact sheet 12 on distance learning), engage in cultural discussions, meditate, do yoga – almost any activity is available online.

ETHICAL CONSIDERATIONS AND RISKS

- By having access to constantly updated, quality information, citizens are in a better position to exercise their fundamental human rights. However, we must remain wary of the negative effects that technology could have on these rights, in particular:

- Not everyone has equal access to information. The digital divide describes today's two-tier society and the gap between the information "haves" and "have-nots". If the situation continues, democracy will be threatened as the less fortunate gradually lose their autonomy of expression. Without direct access to information, we are less able to form our own opinion and can therefore be more easily manipulated by those who are fluent in the use of new technologies. In addition, public sector information is very important for democratic and civic life, and more particularly a key resource for economic activity. If we are to ensure equal opportunities for all, then we need to ensure equal information access and a solid grounding in critical thinking for all.

- Technology and online platforms are not necessarily neutral when it comes to accessing information. Algorithms used by search engines or censorship on social networks shape the information that is prominently displayed.

- Information and communication technologies are playing such an important role in our lives today that soon only those fluent in their use will really be capable of making their voice heard. However, ICTs in and of themselves are only technical enablers and more communication does not mean respect of freedom of expression. Values such as pacific debate and speech, critical thinking and open-mindedness are essential to foster a positive online environment and freedom of expression.

- The huge increase in the means of transferring and exchanging information means that we must take care to protect data about ourselves and therefore our right to privacy (see "Good practice" below).

HOW TO

- In order to become an engaged e-citizen, all users of the Internet should understand their basic rights and responsibilities. Users should understand what they are allowed to do, as well as what industry, government and other Internet users are allowed to do.

- A basic understanding of cookies and how other websites are able to collect and use your personal data is essential (see Fact sheet 9 on privacy).

- In order to avoid complicating the issues for young children, the same basic tenets of good citizenship should be simply extended to online activities: respect, kindness and thinking before acting.

---

15. https://en.wikipedia.org/wiki/Electronic_voting

IDEAS FOR CLASSROOM WORK

- Have students examine the United Nations Convention on the Rights of the Child and analyse which sections are directly related to digital rights[16].

- Ask students to choose several Twitter, Facebook and/or Periscope speakers on citizenship and engage in a discussion. Ask the speakers what their point of view is on digital citizenship and the responsibilities of users. Ask students to devise other questions to pose.

- Students should gain exposure to European websites offering support on digital rights. Ask students to perform a review of Council of Europe, European Commission and European digital rights.

- One good resource which could serve as the basis for your civics study programme is the Council of Europe's online human rights activity programme[17]. You could also ask your class to draw up a human rights charter of its own. Let them apply their new knowledge about human rights to virtual environments, for example how they could make the Internet a better place for them to work and play.

- As part of a history programme talking about the French Revolution, help your students to distinguish facts from hypotheses by comparing heroic revolutionary paintings of the storming of the Bastille with modern accounts. They should be able to "explain how and why the storming of the Bastille has been interpreted differently". This could be linked to media education concepts, such as how reality is represented for different purposes, and the reliability of evidence.

- As part of a geography project, for example "Passport to the world", invite students to discuss the ways in which places of the world are represented on the Internet and analyse how the websites differ in emphasis or attitude with regard to a particular place.

- To help students learn about content analysis, choose a topic, then look it up on news sites from different sources and analyse them in class. Do different organisations use different approaches? Why do you think this is so?

- As mobile phones are an integral part of students' life outside the classroom, examine in class the way they can be used to gather community information and actively participate in democracy. List the services they make available and discuss their effect on privacy and democracy (see Fact sheet 5, "Internet on the go", for information about mobile services).

- Simulate an online debate by posting a message on the blackboard and distributing post-its to students. Each student will be assigned a number and will be able to come up and read the post after a set amount of minutes corresponding to his number. After having read the original post and listened to any forthcoming comments, students will be allowed to write and post their own comment and monitor the discussion to "reply" to other posts. Students will also have the choice of "supporting" a post from another student, which will be placed more prominently next to the original post. This exercise aims at teaching students how an online debate differs from a debate in real life and also addresses the questions of "freedom of expression" and avoiding falling into flaming or other inappropriate online behaviours.

---

16. http://web.archive.org/web/20160501101507/http://blogs.lse.ac.uk/mediapolicyproject/2014/09/12/sonia-livingstone-digital-media-and-chil-drens-rights
17. https://www.coe.int/t/dg4/youth/Training/Training_courses/HRE_Youth_Programme_en.asp

GOOD PRACTICE

- Every citizen has the right to control their own personal data, which necessitates knowing what personal information has been gathered about them. The General Data Protection Regulation was introduced in the European Union in 2016 in part to help citizens exercise these and other fundamental rights related to privacy and data protection[18]. The key points for citizens are summarised in a European Commission press release on 15 December 2015[19].

- Always read the fine print on questionnaires to see how the information you give about your-self is going to be used, and do not forget to consult Fact sheet 9 on privacy for more advice.

- Communication of literacy skills and the transfer of these across school, higher education and into civic society is essential if participation in the democratic process is to increase.

- Consider taking an online course in digital citizenship or digital rights.

- A number of schools are currently working on Internet proficiency programmes in an effort to ensure that their students develop the skills necessary to live, work and play in the infor-mation society of today. These include:

  ► skills for navigating in the labyrinth of information available on the Internet;

  ► developing the capacity to discriminate between information and misinformation;

  ► analysing information for relevance and validity;

  ► understanding the ethical implications of online tools on democracy;

  ► using information in project-based learning;

  ► understanding and using the multiple opportunities that a browser and the Internet can offer.
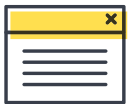
FURTHER INFORMATION

- For information on the General Data Protection Regulation, see: *<http://ec.europa.eu/justice/data-protection/reform/index_en.htm>*.

- The EU Youth Manifesto is an online "declaration" by European youth on how to make the Internet better: *<http://www.youthmanifesto.eu>*.

- For more information on European digital rights, see: *<https://edri.org>*.

- Amnesty International at *<http://www.amnesty.org/>* and Human Rights Watch *<http://www.hrw.org/>* are non-governmental organisations that campaign for human rights. Amnesty has a multilingual manual for teachers called "First steps", designed to help young people learn about human rights, particularly in central and eastern Europe.

- The European Commission has information on protecting children and human dignity in audio-visual services: *<http://ec.europa.eu/avpolicy/index_en.htm>*.

- More information on children's rights can be found in the UN Convention on the Rights of the Child: *<http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>*.

- The Code of EU Online Rights is the basic set of rights and principles enshrined in EU law that protect citizens when acceding and using online networks and services: *<https://ec.europa.eu/digital-agenda/en/code-eu-online-rights>*.

---

18. http://ec.europa.eu/justice/data-protection/reform/index_en.htm
19. http://europa.eu/rapid/press-release_IP-15-6321_en.htm

- For nine elements of digital citizenship, see: *<http://www.digitalcitizenship.net/Nine_Elements.html>*.

- The Paris Declaration, adopted by the European Commission and the European Council of Ministers in 2015, promotes citizenship and the common values of freedom, tolerance, non-discrimination and inclusion through education: *<http://ec.europa.eu/education/library/study/2016/neset-education-tolerance-2016_en.pdf>*.

- Relevant Council of Europe documents include "Human rights for Internet users": *<http://www.coe.int/en/web/internet-users-rights/guide>* (key topics below):

  ► access and non-discrimination

  ► freedom of expression and information

  ► assembly, association and participation

  ► privacy and data protection

  ► education and literacy

  ► children and young people

  ► effective remedies and redress.

Digital parenting: positive and proactive
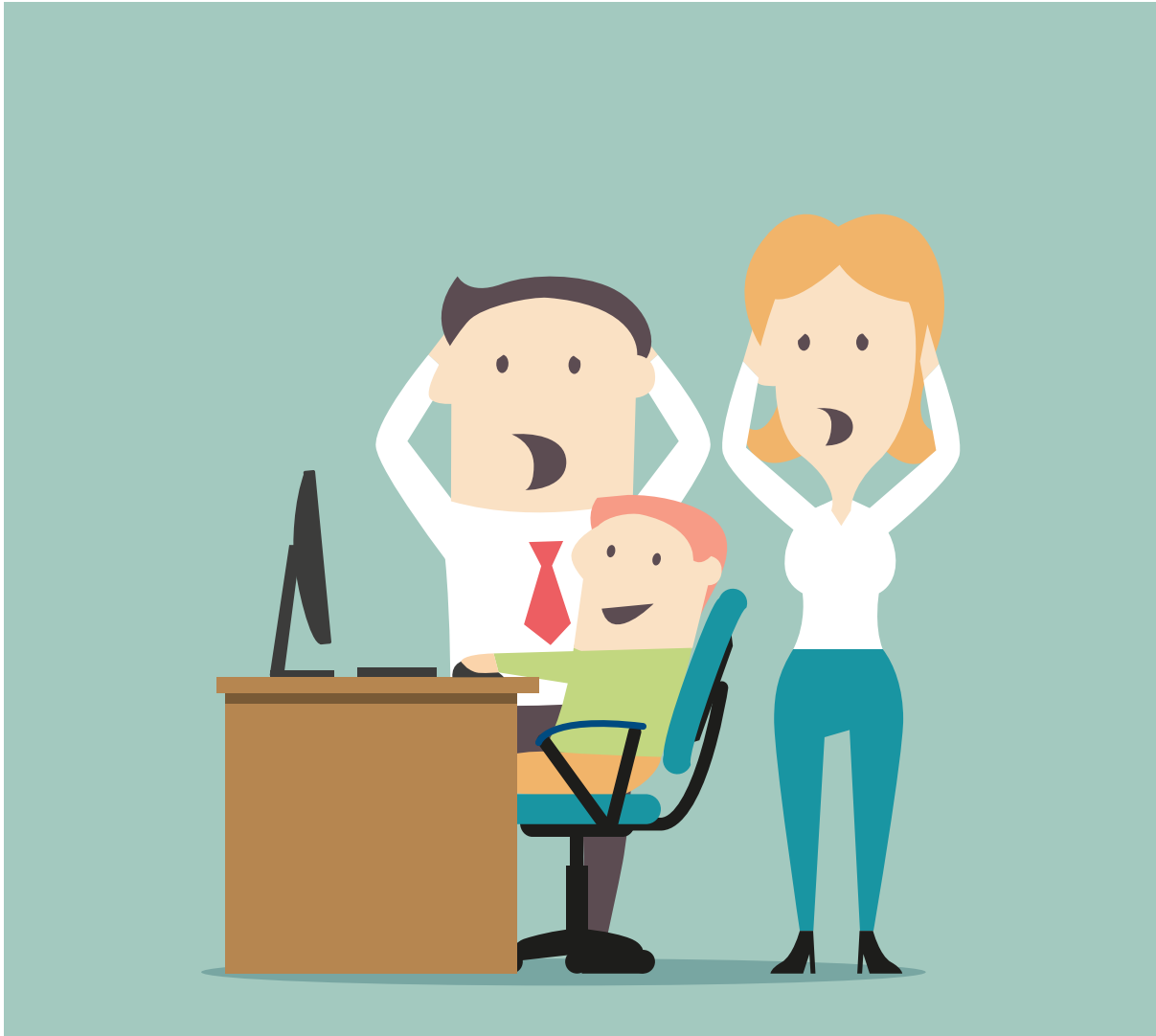
■ **"Digital natives"** are children who are born in the digital age, this age of technology. They are children who, after just a few minutes spent holding a tablet or smartphone, feel no fear or trepidation in manipulating the technology. They swipe, pinch, poke without always understanding what they are doing, but with the confidence that something is happening on the screen. According to Marc Prensky, "our students today are all 'native speakers' of the digital language of computers, video games and the Internet" (Prensky, M. (2001) "Digital Natives, Digital Immigrants Part 1", *On the Horizon* 9(5) pp1-6, 1. Available at: <*http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf*>).

■ **"Digital immigrants"** are people who were born before the advent of technology. It is a phrase also coined by Prensky in 2001 and used to describe the generation of people who did not grow up in the Digital age. Again Prensky describes it perfectly by saying: "Those of us who were not born into the digital world but have, at some later point in our lives, become fascinated by and adopted many

or most aspects of the new technology are, and always will be compared to them, Digital Immigrants" (Prensky (2001), 1-2 <*http://web.archive.org/web/20160413070431/http://www.marcprensky. com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf*>).

▬▬ "Digital parenting" is the notion of guiding "digital immigrant parents" in understanding what their "digital native children" are doing today. The only goal is to protect children, empower parents and keep the communication open between both parties.

Digital parenting is:

- open communication with your child about Internet risks and benefits;
- regular involvement in your child's Internet activities;
- active protection of your child's digital reputation and digital identity;
- learning with your child the opportunities that the Internet can present;
- protecting your child from the dangers that the Internet may pose;
- bringing your offline parenting skills to the online world.

Positive parenting is:

- providing your child with positive discipline and positive guidance;
- bringing up your child to be well-behaved, without being harsh;
- teaching your children from an early age how to behave appropriately, showing them the repercussions of "bad" behaviour and the benefits of "good" deeds;
- being clear about what you want your children to do;
- setting specific and appropriate boundaries;
- demonstrating consistency across the board.

▬▬ There is a clear crossover as the digital parent and carer need all the tools available in order to be proactive, positive and ensure that their child is using Internet and Wi-Fi enabled devices in a responsible manner.

IMPORTANCE IN UNDERSTANDING THE ISSUES

- With the ubiquity of Internet, mobile phones and Wi-Fi connected devices, parents may feel frustrated by their lack of concrete technical knowledge and expertise. And for those parents who are "tech-savvy", they feel concerned by the speed in which their children are embracing the Internet and technology.

- Parents may not know how to deal with children who spend hours playing Minecraft while on a sleepover, or how to set limits on a 17 year-old as regards texting in the evenings, or whether to use a potty-training app to guide their 2 year-old. The questions are endless as technology forges ahead and devices become more streamlined and tech savvy.

- As family structures change, parents may have difficulty maintaining the same technology rules in their partner's home, grandma's home or some other familial environment.

- As technology advances, research on child development and the implications of online use is also advancing, but long-term findings will not be available for a few years yet.

ETHICAL CONSIDERATIONS AND RISKS

- Initial research has demonstrated that using a smartphone or device to "sooth" children may hamper their ability to self-regulate[1].

- Raising a child today simultaneously includes raising a responsible digital citizen, as children need to know how to use the Internet and technology safely and wisely.

- Parents should help their child understand digital literacy: the ability to use information well, the ability to use media and digital technologies effectively and the development of digital citizenship.

- The digital world and the Internet have a profound impact on "offline" parenting as well. Seeing the "online" world as separate from the "offline" world is a misconception. With the endless possibilities offered by the online world, children may encounter certain content or experiences at an earlier stage than they would in the "offline" world. That includes "positive" content such as learning to read earlier, learning music, being exposed to a foreign language and so forth. At the same time, children may also be exposed to sexually explicit content, violence, fear, bullying and similar.

- Beware of the commercial side of the Internet. Most of the online services that are "free" rely on opaque business models and cost structures or exploitation of personal data for advertising. Certain "freemium" games, for instance, will entice your child to spend a lot of money to advance in the game, while "advergames" blur the boundary between game and advertising by discretely associating a product or brand inside a game.

- For nine elements of digital citizenship, see "Digital citizenship: using technology appropriately"[2] and read Fact sheet 17 on digital citizenship.

- The findings from recent studies by the Joint Research Centre of the European Commission, focusing on the use of technology by families with young children, are helpful in understanding the issues and risks[3].

- EU Kids Online is now dedicated to reporting on parental concerns across Europe in its parenting blog[4].

HOW TO

- Be a role model for your children and place limits on your use of technology.

- Stay informed about the latest online issues and discuss your children's online activities.

- Speak with your children's school to determine if there is an online safety programme in place.

- Be careful when removing devices from your tween or teen as a disciplinary measure as this may have unintended consequences, isolating the child from their social connections and networks.

- Speak with other parents to gather good practices at every age.

- To teach your children how to balance their time online, use time restrictions online in the same way as you would teach them to budget pocket money. Give them a set amount of time that they can "spend" each week and let them manage it.

- Stress the importance of offline family time and maintain your weekly family activities.

---

1. http://web.archive.org/web/20160424230408/https://www.theguardian.com/technology/2015/feb/01/toddler-brains-research-smartphones-damage-social-development
2. http://www.digitalcitizenship.net/Nine_Elements.html
3. http://publications.jrc.ec.europa.eu/repository/handle/JRC93239
4. http://web.archive.org/web/20160415215157/http://blogs.lse.ac.uk/parenting4digitalfuture/2015/06/26/svenjas-post-on-little-kids-european-comparison/

IDEAS FOR CLASSROOM WORK

- Ask the students to write a short blogpost to their parents providing tips on parenting in the digital age.

- Engage in a discussion with students about the use of technology today. What are the benefits? What are the risks? Is there anything that the students can do to promote the benefits and counteract the risks?

- After a discussion on good practices when using the Internet, ask the students to list their top tips to share with their younger siblings, nieces, nephews or younger neighbours. How can younger children learn from the experiences of the students?

- Ask students to consider technology in the 1960s and technology today. Did parents have the same concerns? Why? Why not?

GOOD PRACTICE

- Talk to your children about who they are talking to online, what they are doing online, where they are going online and when they are going online.

- Keep the dialogue open – even when the subject may be uncomfortable for you – as it is the best way to stay informed about your child's online activities.

- Alongside the "safe sex" talks with your children, consider having a "safe tech" and a "safe content" Internet talk, and explain the inappropriateness and risks of sexy or extremist photos, talk or messages.

- Be ready to discuss issues such as violence, flaming, bullying, sexuality, gender stereotypes and roles, as your children may encounter these unexpectedly online and will need your guidance to develop resilience and adopt a positive online behaviour in response.

- Understand how to use privacy settings and explain to your child how to put them in place and why it is useful to do so.

- Inform yourself about the business model behind the games, services or websites your child uses. For younger children, make sure that the content is advertising-free, with no hidden costs or "premium" features. It is better to pay a small fee for a game or monthly subscription to a quality service, than expose your child to commercial exploitation attempts.

- Make sure that your children understand the business models behind the services or games they use, or the content they read.

- Make sure your children are not over-sharing (personal information, identifying characteristics, inappropriate photos, etc.).

- Find a healthy balance regarding Internet use and screen time and be a good digital role model yourself.

- Remind your children that anything they write, post or share will exist indefinitely on the Internet – and that it can also be modified and sent around.

- Teach your children how to use reporting tools, so that they can flag any inappropriate content.
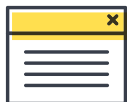
FURTHER INFORMATION

- For information on the effect of iPads on a child's development, see the news report: *<https://www.youtube.com/watch?v=VrQhmcPrhFw>*.

- To read Marc Prensky's "Digital natives, digital immigrants" (2001), see: *<http://web.archive.org/web/20160413070431/http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>*.

- COFACE, the European Confederation of families provides helpful information for families: *<http://www.coface-eu.org/>*.

- The Parent Zone is a UK site that offers a wealth of information: *<http://www.theparentzone.co.uk/>*.

- Check out the publication of the Family Online Safety Institute: *<https://www.fosi.org/good-digital-parenting/>*.

- Vodafone has put out guidelines for parents as well as digital parenting magazines: *<https://www.vodafone.com/content/parents/howto-guides.html>*.

- Boston University Medical Center has published a report on mobile use: *<http://web.archive.org/web/20160607121811/http://www.eurekalert.org/pub_releases/2015-01/bumc-mai013015.php>*.

- European Commission Joint Research Centre has published a report on young children and digital technology: *<http://publications.jrc.ec.europa.eu/repository/handle/JRC93239>*.

- "Play and learn: being online" contains activities for 4-8 year-olds to support parents and teachers in talking with their children about responsible use of the Internet: *<https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=198308>*.

- Guide your young children to sites adapted to their age; there are a wide range of such sites including "Junior: safe search for kids" *<https://www.juniorsafesearch.com/>* and YouTube Kids *<https://kids.youtube.com/>*.

- Relevant Council of Europe are included under the Council of Europe webpage on "Children in the digital environment" *<http://www.coe.int/en/web/children/the-digital-environment>*.

5. Internet – Addressing the challenge

" "To deny people their human rights is to challenge their very humanity."

Nelson Mandela, Nobel Peace Prize laureate of 1993, anti-apartheid activist, President of South Africa 1994-1999

"The rights of every man are diminished when the rights of one man are threatened."

John F. Kennedy, President of the USA 1961-1963

CHECKLIST FACT SHEET 19 – CYBERCRIME: SPAM, MALWARE, FRAUD AND SECURITY

Have you set up strong different passwords for your accounts and configured two-factor security?

Have you explored security settings for your devices/accounts?

Are your operating system and your applications up to date?

Have you made a backup of your most important data?

CHECKLIST FACT SHEET 20 – LABELLING AND FILTERING

Have you thought about the cultural and moral implications of filtering?

Do you know the difference between a "black list" and a "white list"?

Are you familiar with the most commonly used labelling systems for children's content, and what they signify?

CHECKLIST FACT SHEET 21 – ONLINE HARASSMENT: BULLYING, STALKING AND TROLLING

Do you have a clear family or school policy in place so that children understand the repercussions when they are involved in online harassment?

Do you protect your personal details sufficiently? Many online problems are caused through ill-advised sharing of photos and information.

Have you investigated how to build better social and emotional skills (otherwise known as social literacy) to overcome the anonymity and "facelessness" of online communication that facilitate bullying, trolling and harassment in general?

CHECKLIST FACT SHEET 22 – GETTING ASSISTANCE

Do you and your children/pupils know where to report illegal content?

Do you ever check statistics reported by helplines to understand emerging trends and risks?

What are the top five digital skills that will best protect you online?

Do you understand geolocation and Bluetooth sufficiently to use your mobile devices comfortably and safely?

M-learning and mobile wallets are areas in which the use of mobile devices is changing the way we learn, work and shop. What do you know about these recent evolutions?

Cybercrime: spam, malware, fraud, security

While the Internet is a great way to access quality content and services, it can also serve the purpose of ill-intentioned people by disseminating spam, viruses, malware and scams.

- **Cybercrime** comprises offences against computers and data, for example illegal access to a computer (also called hacking), interception of a communication, preventing a computer from functioning or damaging or deleting data, but also offences committed by means of computers, such as fraud or sexual violence against children. Malware, spam and phishing and other forms of identity theft are some of the tools used by cybercriminals.

- **Malware**[1] is an umbrella term used to refer to a variety of forms of hostile or intrusive software, which includes viruses, trojan horses and others. The objectives of malware are very diverse. They can aim simply to disrupt the functioning of your computer by damaging the software or corrupting the hardware, or they may steal information and data which can be monetised in some way or

1. https://en.wikipedia.org/wiki/Malware

another. Your infected computer may also become a "bot" that is controlled by criminals without your knowledge; it may then be used together with millions of other infected computers as part of a "botnet" to spread spam, commit fraud, or carry out attacks against hospitals, airports or banks.

- **Spam**[2] refers to the mass mailing of unsolicited messages to multiple recipients. It is most commonly associated with e-mail, but also applies to social networking, instant messaging, mobile phones and so forth. Fortunately, most e-mail services have efficient spam filters. Spam may also serve as a vector to spread different types of malware, for example when a recipient opens an attachment or a link indicated in the spam mail.

- **Phishing**[3] derives from "fishing for passwords" and is one form of identity theft. For example, recipients receive spam, which is disguised as legitimate mail from a known institution such as a bank or a social network. These mails often contain links to false websites, which are used to gather sensitive user information such as credit card numbers or passwords. The stolen identity information is then often used to commit fraud.

- **Internet fraud**[4] has greatly developed over the last few years as the possibilities for e-commerce and making payments online have multiplied. Internet fraud encompasses different types of fraud such as counterfeits, real estate fraud, premium service SMS ring tones, money transfer fraud and so forth.

SO HOW CAN YOU STAY SAFE?

Your online security can be compared to security at home. You protect the contents by keeping the windows closed and the door locked. A healthy degree of scepticism, critical thinking and ICT skills will also help in preventing you from falling for fraud, phishing, malware or scams online.

Many of the issues relevant for security are also relevant for privacy (see Fact sheet 9).

PERSONAL DEVELOPMENT AND EDUCATIONAL VALUE

Security is as important for your sake as for the sake of all Internet users. Malware, viruses and spam spread mostly through users themselves! If your computer or device is not safe, all your friends and contacts might be exposed to security risks as well!

Knowledge about Internet security and safety is very valuable for the further development of digital literacy skills, as it pushes users to dig deeper into the parameters and settings of their devices and the online services they use, and to gain better technical knowledge about how their devices, their operating systems and the Internet works.

POTENTIAL RISKS

Spam

- Spam is usually benign and the consequences are mostly a great loss of time by having to sort through it, or time wasted clicking on links.

- Spam often includes false or fraudulent information. Because the sender remains anonymous, it is usually not possible to prosecute for false claims.

- Spammers often prey on the goodwill of recipients in order to gather mail addresses for their databases. For example, mails may be sent requesting recipients to add their personal information to a list in order to support a petition or cause. Often citing a cause such as a sick child requiring surgery, it falsely claims that a company or organisation has promised that money will be paid each time it is forwarded.

2. https://en.wikipedia.org/wiki/Spamming
3. https://en.wikipedia.org/wiki/Phishing
4. https://en.wikipedia.org/wiki/internet_fraud

- New techniques of spam appear every day. For instance, on social networks, spam can take the form of "click jacking"[5], with posts shared by friends that include catchy titles such as "the top 10 ways to lose weight" or "you won't believe what this girl does in front of her webcam". The consequences can be that you visit a website that exposes you to a ton of advertising to generate revenue, or forces you to like a page that will spam you with many more posts.

- There are many types of online fraud and new ones appear every day as technology evolves. A common fraud is called "419", named after a Nigerian law prohibiting this type of victimisation. This typically involves promises of a share of a large sum of money in return for help with bank transfers. Another fraud consists in asking the victim to send money as a rental deposit guarantee via Western Union before visiting an apartment for rent.

Phishing and identity theft

- The risks of falling prey to phishing and identity theft are much more serious. Depending on what information you have provided through the phishing attempt, the detriment can be anything from losing control of a relatively unimportant online account such as an online forum to losing control of extremely important accounts such as your main e-mail address which can then lead to all of your online accounts being compromised!

- Once your accounts have been compromised, your data can be at risk. The contents of all your e-mails can be downloaded for instance. This data can prove to be very valuable, either for extorting money from you or your contacts, using your accounts online to order items, using your credit card, impersonating you online, etc.

Malware

- The risks of installing malware are akin to phishing and even spam or worse. Malware can be used for phishing purposes to steal information about your accounts (using a key logger[6] for instance), for spamming purposes to bombard you with pop-ups, notifications or default home screens inside your browsers, and also for other purposes, such as stealing information and data directly from your computer or disrupting the functioning of your computer, taking control of your computer to commit crimes, activating microphones or cameras of your devices to spy on you, and potentially destroying the content altogether.

- Techniques aimed at fooling the user into installing malware are developing rapidly as well. An example is a fake pop-up window which realistically emulates an antivirus scan of your computer. At the end of the fake scan, dangerous viruses are supposedly identified on your computer, and to get rid of them you must install a software – which is actually a Malware or virus!

IDEAS FOR CLASSROOM WORK

- Ask the children and young people to work in groups of three or four and propose a strong password for a fake online account. Make it clear that they should come up with a new password and not an existing password that they already use! Have the different teams present their password and ask the rest of the group to identify the features of a strong password by looking at the proposals.

- A strong password:

  ► is at least eight characters long;

  ► does not contain a word found in a dictionary, does not contain a reference to your personal life or your user name, real name or company name;

  ► contains characters from each of the following categories: uppercase letters, lowercase letters, numbers and symbols.

---

5. https://en.wikipedia.org/wiki/Clickjacking
6. https://en.wikipedia.org/wiki/Keystroke_logging

- A CERT (computer emergency response team), also known as CSIRT (computer security incident response team) is an expert group that handles computer security incidents. Have your students find your national CERT/CSIRT and find out more about the role and functioning of these teams.

- Victims of cybercrime often do not report the crime to the police, and so offenders continue with their business and find new victims.

► Ask your students to find out about how to report a crime to the police or other public authorities, including through hotlines.

► Ask your students to find out what constitutes cybercrime under the laws of their country.

GOOD PRACTICE

- One of the consequences of Internet users expecting to get everything online for "free" has been the continuous development of malware or spam attached to "free" software or services that are used online. The online environment is a shared responsibility and is the result of users' individual online behaviours and choices. By financially supporting quality services/content/software (via donations for open source endeavours or purchasing licences or subscriptions to commercial organisations) you contribute to making the online environment safer.

- User friendliness can be the enemy of security. For instance, you can configure your operating system to ask for an administrator password whenever an important action is performed (for example installation of new software). It can be extremely frustrating and tedious, but that is the price to pay for more security! Keep that in mind when setting up your operating system's security settings.

- If you are managing more than one user of a computer or network, make sure each user has appropriate rights. Restricting unnecessary user rights can help avoid accidental or deliberate security problems.

- Make sure you trust the source before downloading anything to your computer. Be particularly aware of peer-to-peer software[7], which is notorious for aiding the distribution of malware (see Fact sheet 14 on music and images). Whenever you install software, make sure you read all the steps before clicking on the "next" button. Pay specific attention to pre-ticked boxes which may install malware to your computer!

- Install anti-virus software[8] and keep it updated.

- Install security patches or operating system updates as soon as they become available. You can set some operating systems and programs to update automatically or inform you as soon as a patch is available for download.

- Install a firewall[9] to control traffic to and from your computer.

- Use different e-mail accounts for different purposes to avoid giving out your "personal" e-mail address all the time (for example registering on forums, filling out forms, etc.) and avoid distributing your e-mail address on a large scale. Bear in mind that if you include your e-mail address on a website, web crawlers can pick it up and add it to distribution lists for spam. Also, do not respond to spam. This will confirm your e-mail address to the spammer. Be aware that links promising to remove you from their mailing list may not be genuine.

- If you do need to post your e-mail address, you can disguise it by adding characters such as Tom(dot)Smith(at)gmail(dot)com, or posting it as a picture so that it cannot be automatically copied.

- Maintain a healthy scepticism about e-mails you receive. Do not open e-mails if you do not

---

7. https://en.wikipedia.org/wiki/Peer-to-peer
8. https://en.wikipedia.org/wiki/Antivirus_software
9. https://en.wikipedia.org/wiki/Firewall_(computing)

trust the source. Always check the e-mail address of any notification you receive to check whether it is genuine.

- Be especially wary of attachments. If you receive something that looks suspicious, or that you have not requested, delete it immediately without opening it.

- Never click on links from recipients you do not trust, and more especially on links that use shortened URLs where it is impossible to see the "original" URL address. Remember that even recipients that you trust can send you infected messages if their account or device has been compromised.

- Never send or post private information such as a username and password or a credit card number by e-mail. No online service will ever ask you to submit your username and password via e-mail and you will only be asked to share details such as your credit card number on very rare occasions (for example, when reserving a hotel room you may need to send this information to the official reservation e-mail address of the hotel).

- Use different passwords for your most important accounts and be sure to set up two-factor security measures whenever possible (adding your mobile phone number or an extra security phrase/question). Make sure that your passwords have no obvious connection to you, are at least eight characters long and use a combination of letters (lower case and upper case), numbers and symbols.

- Make regular backups of all your data on an external hard drive. Many backup software programs exist and automatically and regularly backup your data. Some of these are even included inside your operating system (Windows, MacOS, Linux, etc.). Be sure to stay informed[10].

FURTHER INFORMATION

- Truth or Fiction is a website for Internet users to check up on claims made by commonly forwarded e-mails: *<http://www.truthorfiction.com/>*.

- Find out more about combating spam: *<http://spam.abuse.net>* and *<http://www.spamhelp.org/>*.

- For information about Microsoft security, see: *<http://www.microsoft.com/security/>*.

- For information on Apple security, see: *<http://www.apple.com/support/security/>*.

- ENISA, the European Union Agency for Network and Information Security gives regular updates on digital security issues: *<http://enisa.europa.eu>*.

- The Council of Europe has a web page entitled "Action against cybercrime": *<www.coe.int/cybercrime>*.

- TechTarget is an information security magazine: *<http://informationsecurity.techtarget.com/>*.

- Helpful information and user tests on topics from cookies to IP addresses to browser checks can be found at: *<http://www.2privacy.com/>*.

- Online security advice from the government of the UK can be found at *<https://www.getsafeonline.org>* and for the United States at *<http://www.us-cert.gov/>*.

- Find your national computer emergency response team through a web search using CERT and your country name.

- Although the information security guidelines offered by the Direct Marketing Association *<http://www.the-dma.org/guidelines/informationsecurity.shtml>* are intended for direct marketers, they also provide useful tips for anyone concerned about online security.

---

10. https://en.wikipedia.org/wiki/List_of_backup_software

- Relevant UN Convention on the Rights of the Child articles:

Article 16 – Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

Article 17 – Children have the right to reliable information from the mass media. Television, radio and newspapers should provide information that children can understand, and should not promote materials that could harm children.

Article 34 – The government should protect children from sexual abuse.

Article 36 – Children should be protected from any activities that could harm their development.

Labelling and filtering

LABELLING

Labelling and filtering are both methods of restricting access to Internet content such as video, images, web pages and games. Despite early hopes from technical and child protection agencies a decade or so ago to create an electronic labelling system that could be embedded into websites for filtering purposes, nowadays labelling usually takes the form of a symbol visible to the naked eye that signifies that specific regulations or standards have been met. However, developing criteria for trust mark and labelling systems, to enable children and their families to identify suitable online content, and sharing international good practice in this area continues to be a priority for the Council of Europe, in particular through the Internet Governance Forum that is organised annually by the United Nations[1]. Labelling of sites is not only a means of protecting minors and increasing public trust in the use of online transactions, it also encourages compliance by content providers with legal standards.

1. www.intgovforum.org

██ PEGI is a European online labelling system supported by the European Commission as it provides guidance on age restrictions and types of content to be found in games and apps (see Fact sheet 16 on games). It provides guidance on age restrictions on games, apps and certain online content as well as an indication of the type of content they contain. It also shows that the content providers respect quality standards which include, amongst other things, obligations to try to keep websites free of illegal and offensive user-created content and undesirable links, to protect privacy and which have an independent complaints mechanism.

██ Quality and trust mark labeling can also be found on shopping and other online transaction sites to indicate that they respect regulations and prescriptions for secure transactions (see Fact sheet 13 on shopping online). One of the most frequent symbols that you may see is the padlock icon, which indicates that the page on the website you are on uses the SSL (secure sockets layer) protocol (a data transfer security standard that encrypts data and authenticates the server and the integrity of the message) or the TLS (transport layer security) protocol. You can therefore reasonably assume that your data, most notably banking details, are secured.

FILTERING

██ Filtering is generally understood as the process of detecting and blocking inappropriate platforms and/or content on the Internet. It can be done within browsers and proxies, or by installing software censors, such as parental controls. Filters are established according to rules set up by parents, schools, businesses, governments and others. They usually function by means of "black" lists (of content to be blocked) or white lists (which bars access to all Internet content except items approved by the filter). Sometimes white lists are brought together within a software system where the carrier or service provider has control over applications, content and media, and restricts convenient access to non-approved applications or content. When such a system is set up for children, it is referred to as a "walled garden" or "closed platform"[2] in contrast to an open platform, where consumers have unrestricted access to applications, content and much more.

██ Another filtering method is when the rules are entered by means of keywords or terms, restricting or completely blocking the access to any web pages containing the banned words or phrases. By means of a password the person who has set the filtering rules can also allow access to sites on an ad hoc basis[3].

██ Today, multidevice filters exist. The filtering software or app can be uploaded to several devices, such as a laptop, tablet, smartphone, television or eReader, and be controlled centrally, for example, by the parent. Different rules can be set for children of different ages and these can automatically evolve with the age of the child. Filtering rules can be applied to restrict time spent online and access to contacts, as well as monitoring geolocation and much more.

EDUCATION

- White lists are especially valuable when children take their first steps on the Internet, enabling them to recognise and quickly access their favourite sites. Not only will this help develop their visual discrimination, a pre-reading requisite, it will also help Internet activities to become shared family activities – a crucial element in ensuring your child's safety online.

- Filtering can be a very useful supplement to shield minors from unsuitable content on the Internet or to monitor usage, but should be used together with appropriate guidance from parents, teachers and child carers.

2. https://en.wikipedia.org/wiki/Closed_platform
3. http://internet-filter-review.toptenreviews.com

- In a classroom situation, filters can be valuable in reducing the risk of students accessing inappropriate or harmful material. However, they do not alleviate the need to check sites to be proposed to students before setting Internet-based assignments.

- The Safer Internet Programme benchmark study (SIP-Bench) shows that today's filtering tools are capable of filtering potentially harmful content without seriously detracting from the opportunities the Internet offers to children and young people. More details are available on the Safer Internet Programme[4] site.

- The issues raised by labelling and filtering practices are rich in material for citizenship and/or social studies themes. Start a debate on the subject of online filtering. Is it an acceptable and necessary form of censorship?

ISSUES

- Content filtering can block access to valuable information and resources, for example to World War history or sex education due to certain key words they contain.

- The labelling and rating of websites remains a largely voluntary practice, except where countries have laws to enforce certain standards. We live in a global world, and their effectiveness is to some extent impacted by their limited take-up by platform and content providers and the lack of common labelling and rating systems.

- Legislation cannot keep pace with technological evolution and still today filtering software services tend to label pages according to their own value systems and social agendas.

- It is difficult to decide what content is actually harmful for children of a particular age, who should decide on the general rules which content providers should observe and who should decide on the application of these rules. Therefore, filtering tools need to be very flexible to enable child carers to shape filtering rules according to the family values. Filter vendors need to develop techniques to ensure they filter in accordance with these criteria.

- Filters can also become a tool of censorship used to shape public opinion and stifle political dissent. Some countries block sites of opposing political parties or ideologies; this can be an interesting starting point for discussing human rights and democracy in class.

- Some people consider filtering as a form of censorship and therefore against the spirit of the Internet. Others claim that if filter software did not exist, governments would be under pressure to regulate online content.

- Filtering software vendors are struggling to keep up with the challenges of social media, mobile devices and the usage of the Internet by increasingly younger children.

- International discussions are ongoing to create a *.kids* domain to replace *.org*, *.com* and similar for sites that are adapted for children in order to guard them from online content that could be potentially harmful, malicious or unsuitable. As sites using the *.kids* domain name would be required to adhere to registration guidelines, the many challenges include setting up internationally acceptable standards, selecting an international monitoring agency and so forth.

---

4. http://www.sipbench.eu

HOW TO

- If you are a game or app developer wanting to have your creation rated according to national or international standards, or a parent or carer simply wanting to understand the process, watch the "how to" video at the International Age Rating Coalition (IARC)[5] website. Most browsers and operating systems have in-built parental controls that you can set to filter out unwanted content. The blog, "How do I set up non-annoying parental controls on all my devices?"[6] provides information on how to do this on a broad range of devices and software. With most filter programs you can specify what types of content you wish to filter or allow. However, pre-installed filters may not fill all of your requirements, especially if you wish to set different rules for two or more users. You will need to purchase a dedicated program for a more sophisticated approach to filtering sites and monitoring usage. The latest Safer Internet Programme report[7] and Internet software reviews[8] can both be useful in choosing from the broad range of products available on the market.

GOOD PRACTICE

- Have a close look at how a filter works before you install it. Does it make any ideological or cultural decisions in its filtering that you do not agree with?

- Use electronic aids with discrimination and do not believe the hype. Test product claims against personal experience. No filter can ever replace the "critical thinking filter" all Internet users need to develop, regardless of their age.

- Talk to students, parents and staff about their usage and needs, and do so regularly. Creating an open discussion environment will do more to add value to your learners' Internet experience than censorship or witch-hunts. Experts recommend that the key to fostering children's responsible use of Internet is for parents to take an interest in their children's online activities and spend time with them online.

- Consider "white listing" options – allowing access only to approved sites – for the youngest Internet users. Bookmark favourite and other child-friendly web sites on your browser to build a personal list for your children so they can easily access safe sites they have used before.

- Children and young people should be encouraged to talk about inappropriate material they find on the Internet. Teens repeatedly claim that one major challenge for them is not being able to speak to their parents about moral issues they are confronted with online. Report potentially illegal content to a hotline[9].

- Monitor your children's activities on gaming websites and look for the PEGI Online label to distinguish safe sites.

- More and more online communities rely on users themselves to help label content, especially when it is user generated. Be sure to label any content that you upload and to help flag content that is inappropriately labelled.

---

5. https://www.globalratings.com
6. http://web.archive.org/web/20160528132556/http://lifehacker.com/5868750/how-do-i-set-up-non-annoying-parental-controls-on-all-my-devices
7. http://www.sipbench.eu/
8. http://internet-filter-review.toptenreviews.com
9. http://www.inhope.org

FURTHER INFORMATION

- Wikipedia has an entry on censorship in cyberspace: *<http://en.wikipedia.org/wiki/Censorship_in_cyberspace>*.

- The Council of Europe media division website gives information on their work promoting self-regulation and user empowerment: *<http://www.coe.int/media>*.

- NetNanny at *<http://www.netnanny.com>* and Cyberpatrol at *<http://www.cyberpatrol.com>* are among the well-known commercial filter products.

- The Electronic Frontier Foundation (EFF) aims to defend civil liberties on the Internet: *<http://www.eff.org/>*.

- The EU-funded SIP-Bench project annually publishes the results of comparative surveys on filtering products in nine languages: *<http://www.sipbench.eu/>*.

- A Council of Europe study on young people, well-being and risk online (2006) explores the meaning of harmful content in the protection of children and young people in the information society: *<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680483b30>*.

- The PEGI Online labelling system website offers information on online gaming, categories, risks, safety tips and a list of labelled websites: *<http://www.pegionline.eu>*.

- Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters: *<https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&direct=true>*.

- Relevant Council of Europe documents: for more information on labelling and filtering: *<www.coe.int/en/web/freedom-expression/internet-standard-setting>*.

Fact sheet 21

Online harassment: bullying, stalking and trolling

As Internet and technology gain a broader reach, so do those people who wish to harm others by harassment.

▬ According to a 2014 study by the Pew Research Center among American adults, there are at least six different forms of online harassment: calling someone offensive names, making efforts to purposely embarrass someone, physically threatening someone, harassing someone for a sustained period of time, sexually harassing someone or stalking someone.In the same study, researchers found five key facts about online harassment:

1. Of those interviewed, 40% of Internet users have personally experienced online harassment.
2. Young adults are the most likely demographic group to experience harassment online.
3. Men and women have different experiences with online harassment.
4. Half of those harassed online do not know who is behind it.
5. Social media was most frequently cited as the scene of harassment.

Online harassment involves directing derogatory or offensive comments at targeted individuals repeatedly. It can take various forms such as cyberbullying, cyberstalking, trolling or spreading hate, for example.

CYBERBULLYING

- The World Health Organization recognises bullying behaviour as "the intentional use of physical and psychological force or power, threatening or actual, against oneself, another person, or against a group or community that either results in or has a high likelihood of resulting in injury, death, psychological harm, mal-development, or deprivation" (World Health Organization - 2002) *World report on violence and health: summary*[1].

- Bullying is an action which is taken against another person in order to cause harm, repeated in various forms over a period of time. Parents and children do not usually have the same perception of the scale of this problem.

- Bullying can take many forms: physical bullying, verbal bullying, relational aggression, sexual bullying, prejudicial bullying, extortion and cyberbullying.

- Cyberbullying is bullying via the Internet or mobile phone, involving offensive or malicious messages, e-mails, chat room or message board comments or, even more extreme, websites built with harmful intent towards an individual or certain groups of people.

- Cyberbullies also use mobile phones to take embarrassing pictures of others or send hurtful SMS or MMS messages. All forms of online bullying have much greater impact than normal bullying since authors are strengthened by a feeling of anonymity and victims have no place to hide from the bully – they can be victims night and day, virtually wherever they are.

- Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, a group or an organisation[2].

- Trolling is the act of causing problems on the Internet by starting arguments or upsetting people, by posting inflammatory, extraneous, or off-topic messages in an online community such as a news group[3] or blog.

- Trolling is done with the deliberate intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion[4].

- Since cyberstalking, trolling and bullying are generally considered under the broader umbrella of online harassment, the guidelines and information below can be adapted according to individual cases.

IMPORTANCE OF RESILIENCE AND SOCIAL AND EMOTIONAL LEARNING

- Social and emotional resilience and well-being are crucial factors to help young people develop protection against bullying and other aggressive online behaviour.

- A positive school climate or a positive community can mitigate on- and offline bullying and, more generally, online harassment.

- Parents can help their children build resilience by helping them increase their self-awareness and self-esteem; by showing them that they are accepted and loved just the way they are; by teaching them to adapt to, handle and overcome tough situations; by inspiring positive emotions, finding pleasure and humour in life; by promoting problem-solving skills; by learning to be flexible in their responses; and by showing them the importance of empathy.

1. http://www.who.int/violence_injury_prevention/violence/world_report/en/summary_en.pdf
2. https://en.wikipedia.org/wiki/Cyberstalking
3. https://en.wikipedia.org/wiki/Usenet_newsgroup>, forum, chat room <https://en.wikipedia.org/wiki/Chat_room
4. https://en.wikipedia.org/wiki/Internet_troll

ETHICAL CONSIDERATIONS AND RISKS

- Bullying and harassment in the classroom can lower the morale of the whole class, creating an atmosphere of fear and distrust, and making learning nearly impossible.

- For those who are bullied or are victims of harassment, the most frequent effects include depression, anxiety, low self-esteem, social adjustment difficulties and loneliness.

- For the perpetrators, the most frequent effects include increased anxiety, risk of school failure, and often delinquent behaviours and an increased likelihood of adult criminality.

- One preventive measure to help keep bullying or harassment from becoming a problem is to introduce social relationship management, anger-management and conflict resolution into your curriculum. Well-chosen programmes of this type will allow children and teenagers to discover their own talents as potential mediators in conflicts. In this way, the risk of minor conflicts developing into threatening behaviour will be reduced both offline and online.

- Your school should have an explicit policy in place – commonly called a responsible or acceptable use policy (RUP or AUP)[5] – to monitor when and how students and staff use the Internet and mobile phones at school. This document should explicitly explain that vulgar, bullying or harassing language and actions will not be tolerated. Direct consequences should be spelled out clearly for anyone who uses the Internet or their mobile phone in an inappropriate manner.

- There should be a procedure in place that can document Internet usage, including who is online, when and where, although this may pose some data protection issues.

- Students should be told to discontinue contact with anyone who is harassing them or making them uncomfortable in any way when online.

- Students should immediately tell a trusted adult what has happened and, if possible, show them the offensive material. Then the adult should follow the procedures spelled out in the school's AUP or RUP.

- The procedure is the same as in real life, were a child to be harassed by someone. They should discontinue contact with the offender and tell a trusted adult about the incident. They should not feel as though they are alone or have to deal with it themselves.

▬ In summary, school Internet and mobile phone use policy should include intervention methods such as conflict resolution, training of students and staff about what to do in the case of harassment online, provision of positive support to the targets of abuse and, wherever possible, help for the abusers in order to change their behaviour. With such a policy in place, schools should have little problem dealing with bullying or harassment.

HOW TO

▬ Educators have always had to deal with bullying and harassment inside and outside of the classroom. It is imperative now to understand how this type of harassment involves the Internet as well.

- Students need to be able to take responsibility for their own actions, but bullying and harassment undermine confidence and self-esteem. When a person is being harassed or bullied, then learning is restricted because he/she is unable to focus, feels threatened and loses self-confidence.

- Students who feel threatened (either online or offline) need the help of a trusted adult. You should also remember that the person doing the bullying or harassing is also in need of guidance so that this behaviour is not repeated in the future.

- Handling bullying and harassment calls for a global approach through open discussion in the family or in class about the nature and potential cause of the unacceptable behaviour and remedial steps that can be implemented collectively.

---

5. https://en.wikipedia.org/wiki/Acceptable_use_policy

- Bullying and harassment are social problems. It is the responsibility of teachers and parents to investigate any allegation of this behaviour and to work in the family or in class to provide the best learning environment possible, whether in the classroom, on the playground or working online.

- Educate teachers on the dynamics of the bullying and harassment process and the ways in which the Internet and mobile phones are used for this. Teach them how to read signals from victims as well as the person responsible for the offensive behaviour, and how to react when they notice such signals.

- Schools should have specific guidelines in place. It would be a good idea to incorporate precautionary measures in your school's Internet policy to deal with bullying and harassment.

- Students should be taught the four golden rules for dealing with cyberbullying or cyber-harassment:

  1. Make a copy of the offensive material if possible.
  2. Do not forward the offensive material to others.
  3. Switch off the receiving device (computer or mobile phone).
  4. Report the incident to a trusted adult.

IDEAS FOR CLASSROOM WORK

- Role play: students participate in a mock conflict resolution process. The teacher assigns the roles and organises groups in which students are responsible for settling a dispute. The next step is to reverse the roles, allowing students to approach the issue from a different perspective.

- Discussion groups: students participate in discussion groups to evaluate their participation in group work, their impressions on topics such as bullying in general, do's and don'ts on the Internet and responsibilities.

GOOD PRACTICE

Here are some ideas on how to handle online bullying and harassing e-mails or messages of any kind:

- Students should be instructed not to open e-mails from unknown sources.

- If an e-mail or text message is opened and found to be offensive, make a copy of the offensive material to show to a trusted adult. However, a victim should never react to offensive messages as this only encourages the other person to continue the offensive behaviour.

- If a person keeps sending offensive or harassing e-mails or messages and it is possible (by means of the e-mail address) to find out where they are being sent from, contact that service provider[6] or mobile operator immediately to report the harassment.

- A school's policies on bullying and/or acceptable user policy should have provisions on how to handle online harassment by students.

- Students should know that they can go to a parent, teacher or other trusted adult anytime they are harassed online or via their mobile phone. It is the role of that trusted adult to take the story seriously and to reassure the victim.

- Deal with bullies or those responsible for the harassment by explaining that their behaviour cannot be tolerated and should stop immediately, but also find out what you can about their motives. Would they dare say or do the same things in real life?

---

6. https://en.wikipedia.org/wiki/Internet_service_provider

- Always endeavour to ensure that parents are aware if their child is being bullied or is a bully him/herself. When a bully uses the Internet or mobile phone to bully, the offensive behaviour does not usually stop at the school gate and will probably continue from home.

- ENABLE[7] (European Network Against Bullying in Learning and Leisure Environments) is a project funded by the European Commission and provides in-depth information on the most successful approaches to tackling bullying, as well as social and emotional learning, and it provides parent packs and peer training toolkits for schools.

FURTHER INFORMATION

- The Council of Europe web page "Beat bullying" offers tools against bullying: *<www.coe.int/en/web/edc/beat-bullying>*.

- NoBullying.com offers bullying and cyberbullying resources: *<http://nobullying.com/>*.

- The Smile of the Child website, based in Greece, offers help with the daily problems children encounter: *<http://www.hamogelo.gr/1.2/home>*.

- "Stomp Out Bullying": *<http://www.stompoutbullying.org>* "Stop bullying now!" is a US website aiming to reduce bullying: *<http://www.stopbullyingnow.com/>*.

- "#DeleteCyberbullying" is an interactive Android app giving advice on cyberbullying: *<https://deletecyberbullying.wordpress.com/app/>*.

- "Know the risks: challenging cyber bullying" is aimed at parents and teachers: *<http://web.archive.org/web/20100923133231/http://www.media-awareness.ca/english/teachers/wa_teachers/safe_passage_teachers/risks_bullying.cfm>*.

- "What is cyber bullying?" is an Australian Government website giving advice to families: *<http://web.archive.org/web/20090703064421/http://www.netalert.gov.au/advice/risks/cyber-bullying/What_is_cyber_bullying.html>*.

- Report bullying and harmful content to the Insafe network: *<http://www.betterinternetforkids.eu>*.

- Pew Research Center has published their 2014 summary of findings on "Online harassment": *<http://web.archive.org/web/20160703044152/http://www.pewinternet.org/2014/10/22/online-harassment/>*.

- The No Hate Speech Movement is a youth campaign of the Council of Europe: *<http://www.nohatespeechmovement.org/>*.

- Find out more about bullying and download lesson plans, parent packs and peer-training kits: *<http://enable.eun.org>*.

---

7. http://enable.eun.org

Getting assistance

The Internet is a global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billion of devices worldwide[1]. It is therefore quite different from other media in that it is the most decentralised medium of communication that exists. It lacks a unique point of control due to the fact that these billions of loosely connected devices have many different routes for allowing communication and transfer of information. In addition, users of online networks are not only viewers but also producers of information since the emergence of Web 2.0 (see Fact sheet 1 on getting connected).

▬▬ Nowadays, as anyone is able to publish just about anything online and a lot of our data is stored in elusive places known as "the cloud", a lot of questions are being asked about the future of the In-ternet and how it can be possible to control even small parts of this flow of information. We often ask ourselves who can determine what speech and information is offensive or dangerous to our children, our family and to us. And more importantly, how can we protect ourselves and our loved ones from it?

---

1. https://en.wikipedia.org/wiki/Internet

ILLEGAL CONTENT

███ Each country defines what content and actions are legal and illegal through its national legislation. Accordingly, the Internet as a means of communication operates as a regulated field. Any action considered to be illegal in "real life" has to be considered illegal on the Internet as well. However, the huge reach of the Internet can amplify breaches of respect for other people's rights and multiply the impact; for example, online "teasing" can become defamation or worse.

███ A broad description of illegal content can be any activity, material, piece of information or similar which contravenes the law and may harm and/or cause prejudice to an individual or entity.

███ Illegal content covers child abuse images and websites, illegal activity in chat rooms (such as grooming), online hate, and xenophobic messages and websites and similar. These and other forms of illegal behaviour are covered by the Council of Europe Convention on Cybercrime[2], the first international treaty on crimes committed via the Internet and other computer networks, and the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems[3]. The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (or Lanzarote Convention)[4] also covers the unauthorised collection and storage of data and mining of information. This Convention is the first international treaty that imposes criminal penalties for all forms of sexual violence against children, including grooming.

GETTING ASSISTANCE IS A FUNDAMENTAL RIGHT!

███ The Internet is a tool that is easy to access from everywhere and by anyone and, therefore, content that is deemed harmful or unsuitable can easily reach children, young people and other vulnerable population sectors. The right to protection against harm and redress against discrimination or violation of any kind is a fundamental human right, according to the Universal Declaration of Human Rights[5]. The UN Convention on the Rights of the Child (UNCRC), moreover, underlines the role of adults to act in the best interests of the child, hence protecting him/her from harmful content and actions, and places the responsibility on governments and families to take all measures to ensure children's rights are respected, protected and fulfilled. This includes providing social services, and legal, health and educational systems to support children and provide an environment where they can grow and reach their potential. Helplines and other reporting mechanisms are an essential element within these systems.

███ Alongside other international organisations, especially within activities in the international Internet Governance Forum, the Council of Europe strives to develop social and family awareness related to the protection of children and young people on the Internet. This includes providing easy-to-find information about the tools and procedures available for obtaining appropriate assistance.

HOW TO

• Illegal content of any nature found on the Internet can be reported to a hotline. A hotline[6] is a service where anyone can make a report of any content suspected to be illegal on the Internet. INHOPE is an association that co-ordinates Internet hotlines in many countries across the world[7]. You can find further information on the type of illegal content INHOPE deals with on their website[8].

• To report illegal content, go to <*http://www.inhope.org/tns/contact-us/details.aspx*> and follow the steps indicated. The hotline will investigate the report[9] to see if the content is illegal and, if so,

---

2. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185
3. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189
4. http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=12/18/2008&CL=ENG;
   http://www.coe.int/en/web/children/lanzarote-convention
5. http://www.un.org/en/universal-declaration-human-rights/index.html
6. http://en.wikipedia.org/wiki/Hotline
7. http://inhope.org/gns/who-we-are/at-a-glance.aspx
8. http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/illegal-content.aspx
9. http://www.inhope.org/en/about/faq.html

trace its origin and contact the law enforcement agencies in the hosting country, as well as the Internet service provider, for removal of that content.

Requesting assistance from a helpline

- Children and young people can request assistance by calling a helpline[10], a service which offers telephone support and/or counselling via e-mail, Web or SMS.

- In many countries, Insafe awareness centres[11] co-operate with national helplines to respond to the questions and concerns of young people linked to their experiences online, or the harmful or illegal online content they encounter. Many helplines that deal with Internet-related problems can also help young people with a broad range of other "real world" issues.

- Child Helpline International[12] is an important contact point in many European and non-European countries. This global network of child helplines operates in almost 150 countries to protect the rights of the child.

- Normally, helplines are open 24 hours a day, 7 days a week. Their services are all free and confidential and they do not trace calls, e-mails or texts. Children and teenagers can write in about a lot of different things and there are facilities to enable young people to communicate via chat, e-mail and forums as well as by more traditional methods. The helpline staff is there to listen and to help them work out their own solutions.

- To find a helpline in your country, you could do a web search with the country name and the words "report" and "helpline".

Using dedicated reporting services on social media platforms

- Most social media platforms, such as Facebook, Twitter, Instagram or Google, have a safety centre to offer guidance to users and an online reporting service to report inappropriate content or activity. This can usually be found under the "Support" or "Help" menu. Reporting instances of bullying, for example, to social networking sites can lead to the removal of the offensive content and even deletion of the accounts of people who have broken the terms of use. Most sites work in similar ways: as an example, on Facebook every piece of content has a drop-down menu which allows users to report a post or photo and say why they do not want to see it. This page contains information about making a report[13].

- All of the mobile operators provide help via phone, webchat or e-mail and many also provide advice specifically directed towards families and children. For instance, Vodafone provides a "Digital parenting" website[14] which provides advice to parents and children and "how to" guides to set up parental controls, as well as offering parental controls and other safety features via SecureNet[15]. The Vodafone Guardian app on Android devices also permits the blocking of unwanted contacts.

FURTHER INFORMATION

- Consult the UNCRC *<http://www.ohchr.org/en/professionalinterest/pages/crc.aspx>* and/or the overview document developed by UNICEF *<http://www.unicef.org/crc/files/Rights_overview.pdf>* for further information on children's right to protection and assistance.

- For in-depth information on protection against and reporting of violence, the Council of Europe's Integrated strategy against violence provides useful information at: *<http://www.coe.int/en/web/children/integrated-strategies>*.

- To report illegal content, you can contact INHOPE: *<https://www.inhope.org/>*.

---

10. http://en.wikipedia.org/wiki/Helpline
11. http://www.betterinternetforkids.eu
12. http://www.childhelplineinternational.org
13. https://www.facebook.com/help/181495968648557/
14. http://www.vodafone.com/content/digital-parenting.html
15. https://securenet.vodafone.com/

- The portal of Insafe, the European network of Internet safety centres *<http://www.betterinter-netforkids.eu/>* offers information on national contact points and helplines across Europe.

- To report cyberbullying or get assistance you can contact Childline *<http://www.childline.org.uk/>*, a free 24-hour helpline for children and young people (Telephone: 0800 1111).

- Befrienders.org *<http://www.befrienders.org>* is a website where you can find your nearest suicide support helpline when in need for assistance.

- Europe Direct *<http://ec.europa.eu/europedirect/index_en.htm>* is a free service where you can get immediate responses to general questions on EU matters and contact details of relevant organisations such as national helplines.

6. Internet - Looking forward

> " "Free expression is the base of human rights, the root of human nature and the mother of truth. To kill free speech is to insult human rights, to stifle human nature and to suppress truth"
>
> *Liu Xiaobo, Nobel Peace Prize laureate of 2010 and human rights activist*

CHECKLIST FACT SHEET 23 – INTERNET OF THINGS

In the same manner that you already protect your computer and other devices from security intrusions, be sure to apply those measures to your "Internet of things" devices.

Be aware that it is difficult to protect every individual device, but that you can protect your network and reduce your areas of vulnerability.

Carefully consider any "Internet of toys" items that you plan on introducing into your home and to your child. Check the security and privacy parameters of the toy and ask yourself: "How necessary is this toy?"

CHECKLIST FACT SHEET 24 – ARTIFICIAL INTELLIGENCE, AUTOMATION AND DISRUPTIVE TECHNOLOGIES

Have you informed yourself about the latest developments in artificial intelligence and automation?

Have you invested in your interpersonal, social and emotional skills?

Have you set up your "smart" devices to ensure appropriate levels of security and user-protection?

CHECKLIST FACT SHEET 25 – VIRTUAL AND AUGMENTED REALITY

Have you talked with your child/student about key topics such as sexism, sexuality, racism, bullying, stereotypes and other forms of discrimination?

Have you made sure that the devices your child/student uses are set up correctly, with high privacy and security protection?

Have you checked that your child/student maintains a healthy life balance when using virtual or augmented technology?

CHECKLIST FACT SHEET 26 – ARE YOU THE PRODUCT? BIG DATA, DATA MINING AND PRIVACY

Have you taken the time to review the way your private data is treated by the online services you use, and to set up adequate privacy settings?

Have you recently reviewed the content you have posted online to make sure that it is still accurate and that you are still willing to share it?

Do you stay informed about the latest developments in "big data" to understand how these changes may affect you and what you can do about it?

Internet of things

The technological advances evidenced by the recent development of Internet and wireless connectivity to data-enabled devices are causing excitement in many areas. This budding field of development known as the "Internet of things" (IoT) where web-connected devices enhance company efficiency and lifestyle convenience may also cause huge concern to parents and individuals alike.

Concerns about security, privacy and data collection are just a few issues that experts and policy makers are trying to address as more and more devices are being designed and sold. However, the IoT presents a special challenge in that experts and policy makers must find unique ways to promote the benefits of this new technology while restricting and even reducing the risks.

Not only do consumers start to ponder when "things start to think", but they must also worry about hackers accessing their "things". Read this recent article "Hackers remotely kill a jeep on a highway"[1] where two hackers remotely play with air conditioning, radio and windshield wipers,

1. http://web.archive.org/web/20160703222843/https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

before cutting the engine on a vehicle. The actions of the two hackers have sparked debate on digital security for cars and trucks.

▬▬ Another area of debate is the idea that the IoT is the next industrial revolution. Today there are an estimated 10 billion connected devices, but estimated growth of this new trend in the market is expected to hit between 26 billion and 30 billion devices by 2020, with an estimated market worth of between US$6 trillion and US$9 trillion[2] .

▬▬ This will lead to an explosion in connected devices and a corresponding explosion in data. The General Data Protection Regulation will face new challenges in protecting privacy, when data is ubiquitous.
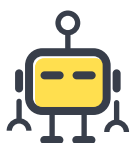
INTERNET OF THINGS

- The term "Internet of things" first emerged in 1999, but it was not until several years later that we saw the real existence of Internet-connected objects.

- The IoT[3] is the network of physical objects or things embedded with electronics, software, sensors and connectivity to enable them to collect and exchange data.

- The IoT is used to describe everything from intelligent thermostats that turn up the heating before you get home to refrigerators that order orange juice when you have run out. People are wearing health and fitness trackers and animals are being fitted with health and location trackers[4].

- The IoT simply means Internet connectivity where devices can talk to each other, making it easier to control and automate tasks – and collect data.

- The Pew Research Center believes that the IoT and "wearables" will have widespread and beneficial effects[5] by 2025.

WEARABLE TECHNOLOGY

- "Wearable technology" or "wearables" are clothing and accessories incorporating computer and advanced electronic technologies.

- Wearables are also called fashionable technology, wearable devices, tech togs or fashion electronics[6].

- Wearables provide instant data to the user and the user is able to instantly monitor the technology, download it for later use or send a printout.

INTERNET OF TOYS

- The IoT can also be applied to toys for children. Wireless connectivity will allow a toy to interact with other data-enabled devices or other toys.

- The Internet of toys is presenting new ways to introduce young people to technology and often encourages them to interact with the toy.

- Hello Barbie, a Mattel Internet of toys venture created in 2015 where Barbie can listen to children, caused concern for parents and privacy experts, as well as leading psychologists, who wonder if these types of toys would cause developmental issues for children, affecting their ability to create, imagine and learn autonomously. ToyTalk, a 2011 company, offers a different opinion and argues that talking toys and Wi-Fi enabled toys can offer learning opportunities to children[7].

2. https://securityintelligence.com/data-protection-in-the-internet-of-things/
3. https://en.wikipedia.org/wiki/Internet_of_Things
4. http://web.archive.org/web/20160310125239/http://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security
5. http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf
6. https://en.wikipedia.org/wiki/Wearable_technology
7. http://web.archive.org/web/20150604014333/http://www.nytimes.com/2015/03/29/technology/a-wi-fi-barbie-doll-with-the-soul-of-siri.html?_r=0

- Despite the convenience offered by the Internet of things and wearables, and despite the diversion and fun offered by the Internet of toys, users may not be sufficiently aware that IoT and toy devices, just like smartphones and computers, may pose security and privacy risks. In the case of toys, there may perhaps even be child-development risks.

IMPORTANCE OF UNDERSTANDING THE ISSUES

The IoT includes wearable devices that many users may not consider as a "computing device"; as such they risk ignoring privacy issues.

The techno-futurist visions of the IoT and wearables are attractive to many. However, the entry-level positioning of the IoT means that more research needs to be done. As cybersecurity firms have learned in the past, people with criminal intent are working harder and faster to create new ways to achieve their end goal.

The advance of toy companies into the domain of the IoT means fantastic new toys for young people, but parents need to understand the risks of having open microphone devices in the hands of young people and open data links in their own homes.

ETHICAL CONSIDERATIONS AND RISKS

The ultimate goal of the IoT is to increase efficiency, but the interconnectivity that accompanies this increased efficiency may pose considerable risks.

- The idea that people can remotely access your devices and your data is a frightening prospect.
- The majority of devices and wearables are not designed with optimal security or privacy in mind.
- Recent intrusions showed hackers viewing people in their homes via baby monitors and webcams[8].
- Consumers may be as "at-risk" of cyber-intrusion as they used to be of physical intrusion in their homes.
- Consumers will need to be aware that the General Data Protection Regulation gives them control over their data and they should inform themselves about how this will work in practice.

HOW TO

- IoT devices vary in design and function. The most important instruction in the proper usage of the device is to read the instructions and to understand the functionalities of the device.
- It is necessary to go through the settings functions in order to disable or enable proper settings that afford privacy where you want it.
- Consider doing research on the device before purchase as some wearables have been recalled or do not function as marketed.
- Remember that this is a developing field and, if you wait a few weeks or months, there is always something newer, better and often less expensive on the market.

IDEAS FOR CLASSROOM WORK

- Have students create a list of all the possible devices that could be connected in a home. Then ask them to list potential security or privacy risks. What can the user do to reduce the risks? What can the device provider do? What can the Internet service provider do?

---

8. http://web.archive.org/web/20160406200102/http://www.bbc.com/news/technology-30121159

- After a discussion on the IoT, ask the students to draft potential instructions to consumers to help consumers understand security issues.

- Read a summary of the General Data Protection Regulation and ask the students to list all the clauses pertinent to the IoT[9].

- Download the video clip on the consumer rights awareness campaign[10] and engage the students in a discussion about consumer rights and the IoT.

- Ask young people to "develop" new toys for the Internet of toys. What are the benefits of the toy? What are the risks? How can they protect young users? How can they reassure parents that the toy is safe?

GOOD PRACTICE

It is important to be open to embracing this new technology, but you should be sure to take appropriate security measures to protect your data and your privacy.

- Restrict personal information on data-enabled devices.
- Reinforce your security on your home wireless network.
- Select strong passwords.
- Where possible, keep certain devices separate from each other.
- Limit Internet of toy interactions with your other devices, and be sure to monitor their capabilities.

Consumers must be attentive to several issues when selecting an IoT device:

- Compatibility and interoperability: is the device compatible with devices from other manufacturers or do you need to stay in the same "ecosystem" to be able to use the device? This is extremely important, as otherwise you will be "locked in" with that manufacturer with no way to switch or integrate other devices from other manufacturers.

- Connectivity: does the IoT device rely only on Internet connectivity to function properly? Ideally, you should be able to access the device without having to connect to the Internet. This is especially important as, if your device manufacturer closes down the online platform for accessing your device, it will effectively become useless.

FURTHER INFORMATION

- More information on EU "Consumer rights and law" can be found at:
  <http://ec.europa.eu/consumers/consumer_rights/index_en.htm>.

- The Guardian has reported on the Internet of things:
  <http://www.theguardian.com/technology/internet-of-things>.

- More information on the Internet of things can be found on Intel's infographic:
  <www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html>.

- Disney has carried out research on the Internet of toys:
  <http://www.disneyresearch.com/project/calipso-internet-of-things/>.

- An Internet of toys guide can be found at:
  <http://www.mutualmobile.com/posts/iot-internet-toys>.

- There is also detailed information from the Children's Digital Media Center:
  <http://cdmc.georgetown.edu/publications-and-papers/textbooks/>.

- Relevant Council of Europe documents: "Human rights for Internet users – Children and young people" *<http://www.coe.int/en/web/internet-users-rights/children-and-young-people)>*.

---

9. <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>
10. <http://ec.europa.eu/justice/newsroom/consumer-marketing/events/140317_en.htm>

Artificial intelligence, automation and disruptive technologies
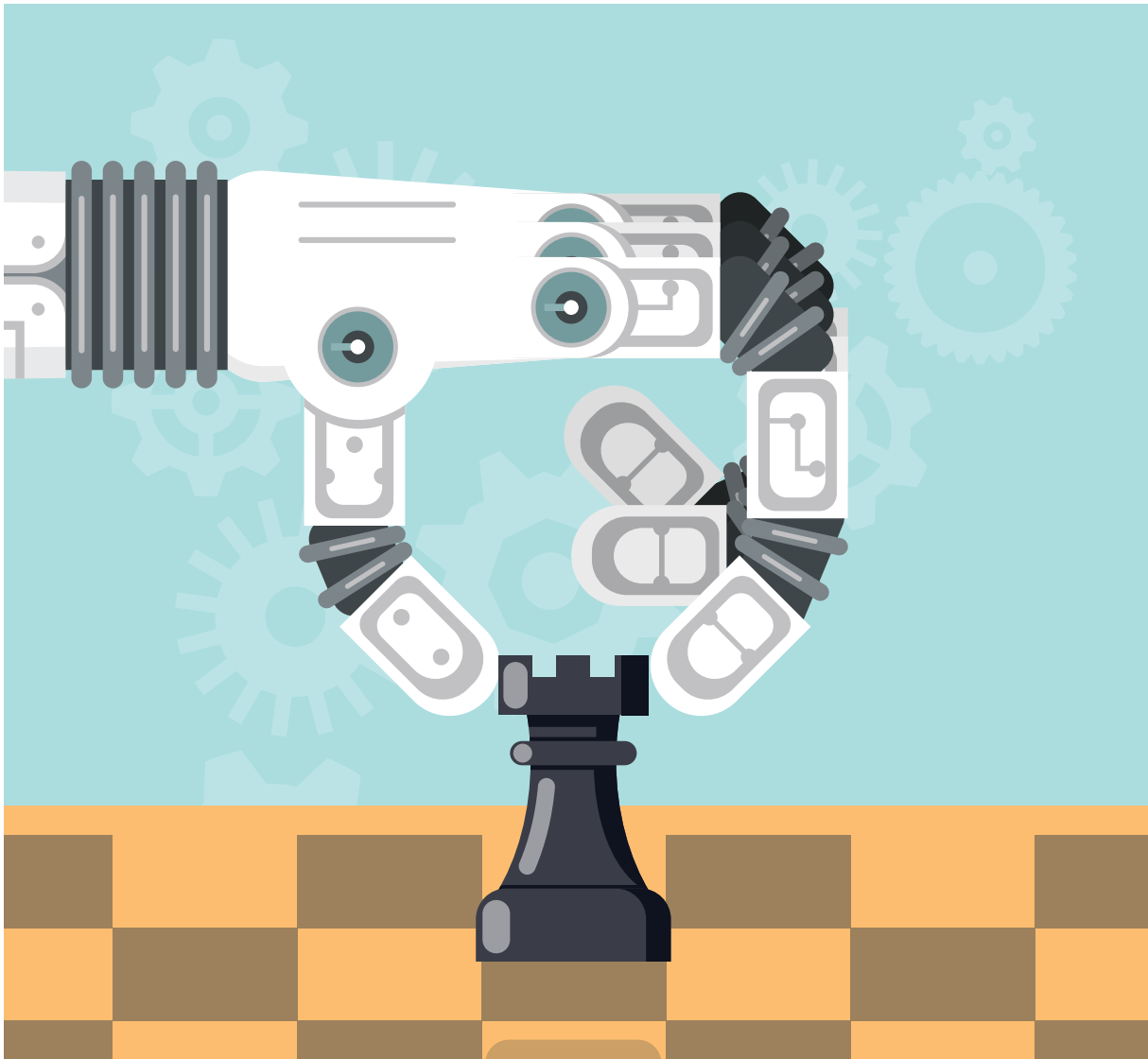
▬ "Automation"[1] is the process by which any action or function operated by a human is replaced by a machine and "artificial intelligence"[2] is the intelligence exhibited by machines or software.

▬ At many points in history, technological leaps have destroyed jobs and created new ones. Take, for example, telephone operators, who disappeared completely as telecommunications technology evolved. Disruptions in the labour market caused by technological revolutions are not a new phenomenon, but each time society fears that there will not be enough new jobs to compensate for the lost ones.

---

1. https://en.wikipedia.org/wiki/Automation
2. https://en.wikipedia.org/wiki/Artificial_intelligence

■ Thus far, such fears have been largely unjustified, as jobs that no one could imagine were created in sufficient numbers to compensate for the jobs lost. For instance, no one envisaged, two decades ago, that there would be such a job as a "social media manager" or a "search engine optimiser".

■ At the same time, current technological developments in artificial intelligence, machine learning and automation are threatening a much larger proportion of the labour market, and not just the low skilled jobs.

NEW DEVELOPMENTS

Self-driving cars

■ Although there is a long road ahead before self-driving cars are available and ready for mass production, progress in this field has been undeniable. Tesla, for instance, already manufactures cars which can drive autonomously on a highway. The follow-up of the very first fatal accident due to a software error in a Tesla car in May 2016 will contribute to determining the future of self-driving technology. The biggest obstacle is not the technology itself but the problem of liability in the case of an accident and the necessary adaptation of the law to situations where machines make decisions in critical situations. But once these roadblocks are removed, taxi drivers, truckers and public transportation drivers (metro, bus, tram) will disappear. In the EU, the transport industry accounts for 4.5% of total employment.

Automatically generated websites, apps, games

■ Web design is a recent profession but it may disappear even faster than telephone operators. Nowadays, with website builders, creating a website has become easier and easier, requiring the user to simply manipulate content by dragging and dropping it on the screen. Complex algorithms are now able to generate your website automatically based on your preferences. "The Grid"[3] is the first service to propose automatic website generation based on your preferences. It just needs pictures, content and some information regarding the purpose of your website and your preferences to generate a fully scalable website (compatible for all screens from computers to smartphones). This is just the beginning. As artificial intelligence, algorithms and machine learning advance, many jobs which required programming skills will be automated, leaving only jobs which require a lot of creativity, customisation or innovation.

Randomly generated art

■ Thanks to advances in machine learning, computers are now able to produce artistic creations ranging from images and paintings to music. Google's "Deep dream"[4] generator analyses your image and shows you imaginary objects inside, much like when you look at the clouds and see a dog or a flower. Other programmes are capable of emulating the style of a painter like Van Gogh or Picasso and applying it to any picture that you have taken[5]. In music, Emily Howell[6] is a programme that is capable of analysing musical scores, inferring the "rules" or "patterns" inside the music, and composing music in a similar genre. While this does not mean the end of artists, it certainly will have an impact on art.

Robots and self-service

■ Huge online retailers such as Amazon invest heavily in robots to carry out tasks such as sorting and organising products or fetching products for delivery. The very first hotel managed entirely by robots has opened its doors in Japan. Self-scanning stations in supermarkets, self-service in restaurants, industrial assembly lines filled with robots, robot assistants in health care and elderly care, automated shipping processes for online shopping and services such as hotels are starting to be managed by robots. More and more examples of automation will be found around the world. Even construction work can be automated with the dawn of 3D printing!

3. https://thegrid.io/
4. http://deepdreamgenerator.com/
5. http://web.archive.org/web/20160114142911/http://arxiv.org/pdf/1508.06576v2.pdf
6. http://artsites.ucsc.edu/faculty/cope/Emily-howell.htm

Predictive and accurate algorithms

▬▬ Thanks to the combination of big data, super computers and powerful algorithms, many sectors such as health care will undergo a new revolution. With massive amounts of health-related data available, algorithms are becoming better than doctors at making a diagnosis based on symptoms, real time sensors and past medical record data.

AI and machine learning

▬▬ With advanced software and computers, it is possible, nowadays, for machines to learn either by observing human actions and deriving certain "rules" or "patterns", and emulating these, or simply learning by doing and inferring "rules" by examining the results of certain actions. For instance, computer programmes have successfully been able to finish video games by "learning" how to beat enemies, jump over obstacles and so forth. There is no telling how much machines will be able to "learn" in the future, but at present it is already clear that repetitive tasks are well within their reach.

EDUCATIONAL BENEFITS

- Learning how to code opens the door to a deeper understanding of robotics and software, including basic AI and automation. This is of utmost importance to identify and sharpen skills that are still outside the reach of computers and machines, and to develop skills that will be needed to push these technologies even further. With low skill and repetitive jobs taken over by machines, there is nothing left but to get more educated.

- At the same time, learning about automation and AI will help shape opinions on policies that will ensure that their impact will benefit society as a whole. For instance, many authors writing about automation and AI advocate a universal salary and lower working hours. A number of scientists, researchers and prominent figures such as Stephen Hawking have signed an open letter calling for a clear direction for the development of AI to avoid being one day enslaved by machines[7].

ETHICAL CONSIDERATIONS AND RISKS

Joblessness

▬▬ The most evident risk of AI and automation is the creation of fewer jobs than they replace. Even though it is impossible to foresee the jobs that might be created as these technologies advance, these new jobs will require highly skilled labour and there will be little opportunity for employment of people with just secondary education.

Growing inequalities

▬▬ As low-skilled jobs get scarcer, there will be a growing inequality between those who have marketable skills and those whose skills are gradually replaced by machines. Another form of inequality will also hit countries with some countries having the technological know-how to make the transition to automation and AI innovations whilst others rely on manual labour. Without proper social, employment and education and training policies, inequalities may stir social unrest.

Over-reliance on machines

▬▬ Automation and AI are no silver bullets. At present, they still require human supervision and only help to complete a more complex task. For instance, while flying an aircraft in autopilot at cruising altitude poses no problems to software, landing and take-off still have to be done manually by humans. However, since human pilots get less and less training and practice, they may be less able to manage a "critical" situation which cannot be handled by an autopilot. The same can be said about self-driving cars. In a future where transportation is automatic, what will happen if the software fails

7. http://futureoflife.org/AI/open_letter

and no human is able to drive anymore? More importantly, if machines end up doing everything for us, and are even capable of creating and repairing themselves, what are we, as humans, supposed to do? This could trigger massive regression of a part of the population which would simply seek entertainment at the expense of sharpening their skills and knowledge which, in turn, would fuel further inequalities and social tensions.

Slow or inappropriate adjustment and development of skills

What automation and AI will achieve in the future is anyone's guess and thus imagining which skills should be promoted because they are "future proof" is a very difficult task. For instance, the world of education is slowly waking up to the idea of teaching programming and coding in schools, but the latest developments in AI show that it is possible to automate programming itself, since it is based on logic and clear rules. The automatic generation of web design is just one example.

Security

As with any device connected to the Internet or relying on software, AI and automation are also vulnerable to hacking. But the consequences could be much more serious than stealing or destroying your personal data. A team of security specialists have demonstrated that it is possible to hack and take over a connected car and carry out actions, such as turning off the engine, or even taking over the steering wheel at slow speeds. Imagine the consequences if a "self-driving" car without a steering wheel was hacked.

The end of dull work, the start of a dull world

Perhaps the greatest challenges posed by AI and automation are philosophical in nature. What makes our world interesting? Can humans be happy in a world which is fully understood, predictable and optimised, with everything running "according to plan"? What about human spontaneity, the deliberate choice to make a mistake and learn from it, or even the right to make an unreasonable decision simply because we can? Introducing "automated" decisions is the logical follow up to our societies driven by science, facts and reason, but is it healthy for humans? Although a century ago, many scientists and intellectuals predicted the end of religion thanks to enlightenment by science, we see now a return of interest in spirituality and religion. Perhaps it is a symptom of a world which is unable to provide humans with a meaning to their lives and is at war with what makes us human: emotions, feelings, impulsiveness and irrationality.

IDEAS FOR CLASSROOM WORK

- A good introductory classroom activity for presenting artificial intelligence, is the so-called "intelligent piece of paper" activity. It consists in presenting a piece of paper with printed instructions on it that can beat any child or young person at the game of noughts-and-crosses (tic-tac-toe). See the detailed instructions here: <http://web.archive.org/web/20160326100226/http://csunplugged.org/artificial-intelligence/>.

- As a follow-up to that basic activity, ask your children or students if they are aware of any artificial intelligence they use in their daily lives.

- Your students will probably have a smartphone and most smartphones come with their own "personal assistants", namely Siri for iOS/Apple, Google Now for Android/Google and Cortana for Windows/Microsoft. All three present characteristics of artificial intelligence: they have a voice recognition feature which gets better as it listens to millions of human voices, they have an algorithm for answering questions you ask and they personalise information they display to you based on the data you feed them (search data, contact details, location data, etc.). The same applies to basic features like predictive typing. This is also AI technology.

- Artificial intelligence, automation and machine learning can be very useful, but never forget to maintain certain manual skills in case they fail. For instance, even if GPS applications are now common on smartphones, it is never a lost exercise to learn how to read a map and develop your sense of orientation.

- Keep everything under control. There are many levels of automation, the most extreme being a machine taking decisions with no input or validation by humans. Just as in predictive typing where the user always has the choice to accept or reject the proposal made by the software, so too should you configure any automated or AI-powered device or software to require your validation.

- Be prepared for change and be versatile in developing many different skills. As these disruptive technologies enter the market, it is the most versatile and flexible workers that will be able to adapt. In the future, it is very likely that workers will have to "retrain" or return to education frequently to develop new sets of skills. Lifelong learning will be the norm.

- Boost your interpersonal, social and emotional skills, as these are safe from any form of automation. While robots and algorithms will be able to replace many low-skilled jobs, they will never be able to replace quality and human interaction.

- AI and automation rely on software. Make sure that any "smart" device that you own runs the very latest software version by regularly checking for updates, and adjust to high security settings. If your device does not require permanent connection to the Internet to function, make sure it is disconnected to lower the probability of hacking.

- In order to connect the dots and have a global overview of what the future may bring, make sure that you read the Fact sheets on big data, augmented and virtual reality and the Internet of things. Understand that big data is what fuels artificial intelligence and automation, that augmented and virtual reality are new ways of interacting with AI and machines, that the Internet of things will be not only another way of interacting with AI and machines, but also a means of feeding them valuable data which will further fuel their development. Only by understanding the big picture will citizens be able to make conscious and informed decisions about harnessing these changes for a better society.
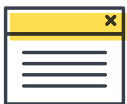
FURTHER INFORMATION

- This is an article about artificial intelligence from the BBC: <http://web.archive.org/web/20160509115227/http://www.bbc.com/news/technology-34224406>.

- Google offers a research page about artificial intelligence and machine learning: <http://research.google.com/pubs/ArtificialIntelligenceandMachineLearning.html>.

- News about automation is available here: <http://www.automationworld.com/>.

- This is the official web page of the Consumer Electronics Show which often showcases the latest innovations in the fields of technology: <https://www.cesweb.org/>.

- News about the latest research and innovation in the field of ICT is available from the EU Commission Research and Innovation Magazine: <http://horizon-magazine.eu/topics/ict>.

Virtual and augmented reality

Virtual reality[1] is an immersive multimedia experience which replicates an environment that simulates physical presence in the real world. The sensory experience created can include sight, hearing, touch, smell and taste, with the first two being most prevalent.

▬ Augmented reality[2] is the addition of computer-generated sensory input such as sound or images to real-world environments.

▬ While the idea of virtual and augmented reality go back several decades, it is only recently that technology has gone far enough to envisage commercialisation of virtual and augmented reality devices, services and software. Augmented reality applications have grown fast through smartphones, mobile Internet and geo-localisation technology.

1. https://en.wikipedia.org/wiki/Virtual_reality
2. https://en.wikipedia.org/wiki/Augmented_reality

▬ Some examples of recent developments in virtual and augmented reality include:

- the increased availability of virtual reality headsets such as Oculus Rift, Samsung Gear VR, HTC Vive or Sony Playstation VR, with a number of games set to launch, notably through the Android and iOS mobile platforms, the PlayStation 4, Xbox One and traditional PC or Mac computer games;

- the increased availability of augmented reality headsets or glasses such as Google Glass and Microsoft HoloLens; Microsoft plans to launch an augmented reality version of Minecraft, playable in your living room;

- the release of mainstream augmented reality games such as Pokemon Go which enables you to catch Pokemons in the real world via your smartphone (iOS and Android).

EDUCATIONAL BENEFITS

- Virtual reality, by its possibility to simulate a real world experience, presents a great number of opportunities for learning. For instance, learning how to drive a car can be accurately simulated.

- Given the level of immersiveness of virtual reality, experiences have already shown promise in using virtual reality for therapeutic purposes, such as getting rid of arachnophobia or overcoming post-traumatic stress disorders (PTSD). It has also been used successfully to increase the level of empathy and understanding of others by enabling a user to experience what it feels like to be in someone else's shoes: being a person with a disability (a blind person, a person in a wheelchair) or being a minority suffering from discrimination.

- Although nothing can replace reality, not everyone has the opportunity to travel. Virtual reality can simulate visiting a monument or any other place "as if" you were physically there yourself. But it can go further and make you visit places you could never normally go, such as the moon or outer space, or the inside of a volcano, or it can even bring you back in time to simulate being on an 18th century battlefield or walking alongside dinosaurs.

- Augmented reality has too many beneficial applications to be listed. Since it consists in overlaying "extra" information or objects on the real world, possibilities are endless. With augmented reality, no need for a tour guide since, as you look at a monument, statue or anything really, useful information can be superimposed over it. Superimposing information has no real limits. It can be a menu or review for a restaurant, reminders about people's names or information about them when you see them, and so forth. In terms of learning, it also carries limitless possibilities: showing you how to fix/replace a car part by superimposing the steps you need to take, helping a surgeon during an operation, showing you how to prepare a recipe by simulating how you should cut your ingredients and how to mix them. Anything you look at can be "augmented" with extra information. A classroom can thus be turned into a stage where virtual objects can be added, showing a semi-transparent model of a human body, for instance.

ETHICAL CONSIDERATIONS AND RISKS

Behavioural risk

▬ A number of studies have looked at the link between playing video games and real-life behaviours such as an increase in violence and aggressiveness. The conclusions, however, are still controversial. Some studies point to "short-term" aggressiveness and violent behaviour after playing a violent video game, other studies underline the "discharging" effect these games have on children. Other details, such as whether the game was multiplayer with an element of co-operation, also affect the results. The truth is that we are still far from understanding the long-lasting effects of video games

on children and young adults. Virtual reality and augmented reality will add a further layer of realism to video games, making it closer and closer to "reality" and little to nothing is known about how this will affect children. Recently, many controversies have surrounded video games such as GTA V where a third-party add-on developed by individuals allowed players to simulate rape on a virtual female character. Sexism in video games is a well-known phenomenon, with female players often pretending to be "male" in order to avoid harassment. And it is not just about the formal content of video games. Live chat through video games has been used for disseminating extremist content, sexism, bullying, hate speech and similar. Video games using virtual and augmented reality will be part of the media that children will consume in the future, and will inevitably contribute to shaping their attitudes and behaviours to a certain extent. Should irresponsible developers feature extremely violent, extremist, sexist, racist, homophobic content inside their games, this could negatively affect users.

Privacy

Augmented reality relies on the permanent real-time analysis of the physical world to accurately "augment" it with virtual elements. This means that your localisation and what you are looking at needs to be fed to supercomputers, usually online, to accurately calculate what should be displayed. Without proper privacy protection, augmented reality could become a way to spy much more deeply on people, in real time.

Security

With devices being connected permanently to the Internet, distance live hacking has become easier. As we will start using augmented and virtual reality devices, such as glasses or even contact lenses, new potentially very dangerous hacking situations could arise. For instance, if a driver uses augmented reality display to provide directions, the display could be hacked to distract him/her from the road.

Manipulation and consumerism

Augmented and virtual reality will also bring with them new advertising strategies. As there is no regulation on what is allowed, the sky is the limit and we can easily assume that techniques such as "augmenting" your home with advertisements will be used. For instance, you could open your fridge and an advertising device would "augment" your fridge's content to display products that you "should" have inside. In the supermarket, while scanning a product with your smartphone, a notification may suggest you buy another product.

Dependency and addictiveness

Neurosciences have taken a leap in recent years and much has been discovered about our brains. The brain takes much pleasure from fast stimuli such as quick action, movement and similar. This is what makes video games and fast-paced action movies so successful. Unfortunately, the "real" world requires the acquisition and practice of skills such as restraint, self-control, patience, perseverance and pro-activeness. Not everything can be "gamified" or made "pleasant" via technology. Learning the violin is just one example. As children will grow up with virtual and augmented reality, there is a risk that they will not be able to cope with a world which is not "augmented" or not as "rich" and stimulating as their "virtual" reality. MMORPGs (massively multiplayer online role playing games) are a good example of this. While they help develop a great number of skills, such as a sense of organisation, planning, leadership and co-operation, they come with a very "enjoyable" learning curve which is just challenging enough to keep players interested, but not too difficult to discourage them. Augmented and virtual reality will exacerbate this problem and might create addictiveness and dependency towards a world in which it is easier to cope, is less frustrating and much more stimulating than the real world.

Loss of interpersonal skills and asocial behaviours

While still a limited phenomenon, in some countries, such as Japan, there is a growing

phenomenon whereby adolescents and adults, referred to as "Hikikomori", withdraw from social life. While not directly related to the media, television or the Internet, these mediums make this social withdrawal more bearable as they provide a distraction from the difficulties of "real" life. Virtual and augmented reality may exacerbate the phenomenon even further, as virtual realities might be easier to cope with and more gratifying than "messy" human interactions. Even sex and sexual relationships come with their share of negative emotions, the pressure to perform, the shame of body image, all of which disappear in a virtual world where the user is in full control of everything.

Physical health

■ Augmented reality and virtual reality also bring an opportunity to solve physical inactivity problems such as users sitting passively behind screens for hours on end. Location-based games, for example, can take place in the real world with augmented reality, and projects can create special rooms for virtual reality environments. At the same time, immersive experiences pose new problems, such as ignoring signs of pain or overuse due to the power of virtual or augmented content to capture our full attention. Repetitive motions inside a game can lead to tendonitis, as seen with some Wii games. Also, motion sickness and nausea can be a strong side effect of the immersive experience of augmented reality, since the images that are being fed to the brain through a head-mounted display clash with the input from motion sensors in the inner ear. Finally, many beta testers have reported getting hurt through falling or colliding with an object, while immersed in virtual reality or even augmented reality, as they have been staring at smartphone screens while playing augmented reality games in the real world.

Harassment, cyberbullying and contact related risks

■ As the boundary between what is real and what is virtual alters, virtual and especially augmented reality could be used as an instantaneous, live way of humiliating someone, for instance by programming the overlay of a rat head upon facial recognition of a person, or sharing a live stream of someone in a humiliating situation.

■ Augmented reality and, to a lesser degree, virtual reality carry "contact" related risks. Massive augmented reality games rely on playing in the real world against real people who are strangers. Problematic situations can include being mugged or assaulted in real life.

IDEAS FOR CLASSROOM WORK

- Augmented and virtual reality rely heavily on hardware. If your school or learning institution is not properly equipped with tablets for instance, then you will not be able to take full advantage of these technologies. In some cases, the devices of children and young people themselves can be used (such as their smartphones) but this poses issues with regards to school policy, as some schools forbid the use of smartphones during school hours, and may lead to discrimination, as some students may not have a mobile phone powerful enough to handle an augmented or virtual reality activity, or may not even have a mobile phone at all.

- That being said, there are many resources available online to help you use augmented and virtual reality in the classroom. Augmented reality is easier to use as it does not require "head gear" that provides a fully immersive experience and will work with existing devices such as smartphones and tablets.

- If you are interested in using augmented reality, you can find a list of tutorials, guides and apps at Kathy Schrock's website "A guide to everything"[3] website[4].

3. http://web.archive.org/web/20160318145342/http://www.schrockguide.net/augmented-reality.html; OnlineUniversities.com
4. http://www.onlineuniversities.com/blog/2012/09/20-coolest-augmented-reality-experiments-education-so-far/

GOOD PRACTICE

- As always, since little is known about the effects of prolonged use or exposure to these new technologies, maintaining a healthy life balance is a must. Make sure that you and/or your child balance your "connected", virtual or augmented activities with "traditional" sports or other hobbies. This also applies to classrooms. Augmented and virtual reality are flourishing businesses and, while many claims about the benefits of using them in education may be true, there is no silver bullet for providing quality education. A healthy balance between traditional and new teaching methods is the way forward.

- Carefully choose the content that you buy for your children should they use virtual or augmented reality devices and keep a check on what they have access to. Read age restrictions and labels, for example PEGI labels (see Fact sheet 20 on labelling and filtering, and Fact sheet 16 on games), and enable parental control tools on devices used by younger children to make sure they cannot access content freely. For younger children, use quality white lists, if they are available in your country/language, as it is the best way to both protect them and ensure that they are exposed to positive content that has been reviewed by professionals.

- It is more important than ever to talk openly about violence, cyberbullying, sexuality, and rights and responsibilities with children and young people. Setting strong ethical standards from the youngest age is the most effective way to neutralise sexist, racist or any other discriminatory or negative message that your children may encounter at some point online or through their virtual and augmented reality devices.

- Set the privacy and security settings at the highest level for younger children. See Fact sheet 9. Remember that these devices are at risk of being hacked.

- Be sure to check the business model behind the content or device that you use for virtual and/or augmented reality, as you or your child might be exposed to intrusive advertising.
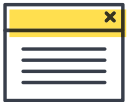
FURTHER INFORMATION

- News about the latest developments in virtual reality is available on Venture Beat: *<http://venturebeat.com/tag/virtual-reality/>*.

- There is an article about virtual reality and education from Stanford University: *<https://teachingcommons.stanford.edu/teaching-talk/virtual-reality-and-education>*.

- News about the latest developments in augmented reality are also available on Venture Beat: *<http://venturebeat.com/tag/augmented-reality/>*.

- General information about augmented reality is available from the Dartmouth College Library Research Guides: *<http://researchguides.dartmouth.edu/AR>*.

Are you the product?
Big data, data mining and privacy

Big data[1] is a broad term that refers to data that is so vast that it cannot be analysed or processed by traditional methods (using one computer or a simple application for instance).

▬ Big data finds its roots in the combinations of:

- an ongoing tremendous growth of digital storage capacity;

- an increase in data generated by our societies (increasingly, everything we do leaves a digital trace);

- an interconnected world via the Internet which enables all that data to be connected together; and

- a growing ability to analyse and make sense of all the data generated.

---

1. https://en.wikipedia.org/wiki/Big_data

▬▬ Examples of online services using big data include social networks such as Facebook, search engines such as Google or Bing, and online retailers such as Amazon. But big data is much more than an "online" thing; it extends into our daily, offline lives too.

- Supermarkets use store cards to analyse shopping patterns and adjust their inventory in real time or programme a special store event (marketing, sale, etc.).

- Data generated from drivers, sensors from their cars and GPS devices help provide real-time traffic information.

- In hospitals, analysing data from sensors, such as the rate of the heartbeat, in real time can help identify infections or other health problems before any external signs and symptoms can be detected.

▬▬ Data has also become one of the most popular online currencies. Instead of paying with hard money for the online services you use, such as social networks or search engines, you "pay" with the data you feed into these services. This data allows services to customise advertising and marketing to your preferences, making them more effective. However, "paying" with data is a poor comparison. As opposed to money, data is much more sensitive. It can be reused multiple times and be resold. A fairer comparison would be to give the key to your house in exchange for accessing a service!

▬▬ We are only at the very beginning of this revolution as data becomes even more extensive via, for instance, the Internet of things (see Fact sheet 23 on the Internet of things), and as data analysis becomes more efficient via an increase in computing power and advances in data analysis techniques (artificial intelligence, etc.).

EDUCATIONAL BENEFITS

- Big data carries plenty of potential to optimise and facilitate many parts of your life: making sure that your search queries are more accurate, that your commuting to/from work or school is as time efficient as possible, that you always find the groceries you want in your local store, and so forth.

- Learning about big data and how it works is essential to harness its power and make sure that it works for, and not against, you. This implies choosing carefully which kind of data you are willing to share and selecting services and products based on their use of data.

- Big data can also serve the purpose of helping to understand our societies, making it possible, for the first time in human history, to analyse and make sense of large masses of data generated by people. For social sciences, psychology, behavioural sciences, health care, marketing and many more areas of research, big data is a real breakthrough. The findings in these fields can be harnessed by teachers to illustrate certain sociological concepts with real-life examples and figures.

- The prevalence of online business models relying on data rather than hard currency as their main source of revenue also creates the need for new skills such as personal data management and privacy protection skills. So, similarly to managing your personal budget and finances responsibly and not overspending, you will also have to learn to manage your personal data responsibly and not overshare.

ETHICAL CONSIDERATIONS AND RISKS

Privacy and data protection

▬▬ While many laws protect individuals' data and privacy, in reality they are difficult to implement. The General Data Protection Regulation (GDPR) requires services to ask for user's explicit consent, but this will most likely only extend the "tick box" exercise, similar to agreeing to "terms of service": either take it or leave it. Users often do not have granular and detailed control over their data and are faced with choices of either sharing everything or nothing. Even if the GDPR tries to address the issue of consumer consent by introducing the principle of proportionality (that is, if the service asking for access to a consumers' data really requires such data to provide the service), the interpretation and enforcement in practice may not be sufficient to protect users. For instance, do social networks require the use of your data for sorting your newsfeed?

▬▬ The very concepts of privacy and data protection will need to be further developed in the years to come. What does privacy mean? Can your data be exploited as long as it cannot be traced back to you? How can you control the extent to which your data is shared and used in more detail, given the sheer amount of data generated by users on a daily basis?

Standardisation, conformism and stagnation

▬▬ Big data is a blessing for optimisation. Public transportation, health care and hospitals, urban planning, all of these sectors can benefit from analysing data generated by users, patients and citizens in order to be more efficient. But what if you are different? What if you go to work at unusual hours, what if you have a unique disease, what if you do not want to conform to the "mainstream" way of life? If all the services around you are designed more efficiently on the basis of big data, you as an individual, along with your unique aspirations and needs, may be left out.

▬▬ But big data can also be used to tailor a service to your needs: search engines, for instance, customise search results based on prior searches and any other data about you; social networks show you posts that you might like. However, showing you only what you want to see, or what you enjoy seeing may have the adverse effect of personal stagnation. For instance, should your political preferences and convictions be more right wing or more left wing, being fed only information and content that supports your views may be flattering to your ego, but might be terrible for fostering core values such as democracy, debate and personal growth – instead it will "lock you in".

Discrimination

▬▬ Whenever you subscribe to a life insurance, apply for a job, ask for a loan or get car insurance, your competences or the risk you present are being assessed. This can be via a health questionnaire asking if you smoke or do sports, a job interview to test your skills or a check on how you have recently managed your budget and whether you have repaid any loan you have taken out. But where is the line between "fair" assessment and downright violation of your privacy? Many employers already use online information about job candidates to make hiring decisions and there are many hints of insurance companies and banks moving towards analysis of online data to assess the probability of your defaulting on a loan or having a serious health issue. While big data can save lives through its predictive powers, it can also prevent some people from having access to basic financial services or health care.

Selling anti-discrimination

▬▬ Online reputation-management companies have started to emerge on the Internet. Businesses and individuals can pay these companies to manage their reputation and ensure that their data does not exclude them from access to certain services, such as credit/investment, insurance or employment. This is an example of a commercial exploitation of an externalities cycle akin to polluting a river, selling medicines to poisoned citizens and paying a business to clean the river.

Manipulation and consumerism

▬▬ Given that the most popular business model for apps and online services alike is the "free" advertising, often based on the exploitation of user data, there is a risk that consumers will be exposed to more and more messages encouraging them to consume. Online advertising is growing each year and new techniques that force consumers to look at or click on advertising are evolving fast. For instance, pre-screening videos appeared only a few years ago. Big data fuels the growth in advertising by making it more efficient and customising it to individuals' habits and interests while learning from mass data the most effective design, place and method for an ad to be seen and interacted with.

Political persecution

▬▬ While some governments respect privacy and do not spy on their citizens, many do not. The revelations from Edward Snowden showed that governments from all over the world spy on Internet users. In some cases, this is justified for security reasons, such as fighting terrorism and preventing a terrorist attack, but the proportionality of such actions always needs to be questioned. For instance, the police may investigate social network profiles to identify citizens present in a protest march.

Consumer rights

▬▬ Big data is the new online currency, but what do users get in exchange? The right to use an online service rigged with harassing and pestering advertising? When users pay a monthly fee for using a service, they are protected under consumer rights laws and are entitled to compensation if the service or content does not meet their expectations or presents serious flaws. A user could get a refund from an online video platform if he/she is unable to watch a movie, but what if your favourite social network has bugs or is unusable? What compensation are you entitled to? After all, the social network has used your data to make you look at advertisements and made money from it. The new business model relying on data as a currency poses many problems to consumer rights; as it is supposedly "free", users are often entitled to no compensation and their rights are very restricted.

The end of anonymity

▬▬ While pseudonyms and nicknames have not yet disappeared, anonymity is under serious threat in the wake of big data. By making links between several pieces of anonymised data, it is possible to identify a person by name online. Even by being very cautious about the information we post, it will be hard for anyone to remain anonymous online in the near future, for better or for worse.

The Internet never forgets

▬▬ The "right to be forgotten" has gained traction since the European Union took legal steps to make it happen. In practice, however, this is still difficult. Digital content can be easily reposted, modified slightly to be unrecognisable by automated Internet bots or moderators, or hosted on online servers or services that are outside the reach of EU law. Everyone can now easily take pictures or videos with their smartphones at any time, meaning that you can no longer make a fool of yourself and act irresponsibly when you are at a festival without the risk of seeing it uploaded online and have the whole world making fun of you. A fine balance still needs to be struck between the right to accountability and the right to be forgotten.

Bad quality content and services

▬▬ As online services and content creators rely more and more on advertising for revenue, they will seek to optimise the attractiveness of their service or content. Big data helps in identifying what makes an article, a photo or a video attractive, but will that work for or against quality content or services? More and more articles online rely on "click baiting" to attract users to click

on the link or post and be drawn to their advertisement-filled page. Titles such as "the top three secrets to lose weight", "you won't believe what this girl does in front of her camera" or "the top 10 cutest cats on the Internet" are found more and more frequently online. While there is nothing wrong with entertainment and anecdotal content, the business model relying on advertising is creating a strong incentive to create only that type of content to the detriment of factually accurate content or educational content.

IDEAS FOR CLASSROOM WORK

For young people 14 years old and above: invite the young people to make a search for their name and/or look through the data already available about them online, then to analyse it from the perspective of an employer, an insurer and a government law enforcement authority. Get them to discuss how they would be seen by these organisations were they to analyse the data available about them. For instance, posts sharing articles about the benefits of procrastination or status updates that contain many spelling mistakes may look very bad from the perspective of an employer. Pictures where you are shown smoking and drinking or doing dangerous activities will look bad to an insurer. And finally, posts criticising your government and calling for radical change may look suspicious to law enforcement agencies.

GOOD PRACTICE

- The Internet and big data, in the end, are just further steps in the technical revolution. Whether the end results are good or bad for humanity and society depends on the uses we make of them. As a citizen and as an Internet user, you can shape the way big data will be used, encourage initiatives that work for the benefit of society and suppress those that go against the public interest. For instance, as a citizen, you can vote for policy makers who promote strong ethical standards regarding the use of data; as an Internet user, you can support services and companies that handle your data ethically and responsibly.

- Stay informed about the latest developments in big data, as these will have deep repercussions on your daily life. Not only will this help you decide upon the data you wish and choose to share, it will also help you identify and support policy makers and companies that are in line with your ethical standards on how your private data should be treated.

- Keep track of all the services that you have used and all the content that you have posted online from the very start of your online presence, especially if you have started young! The comments or posts that you have posted as a child or teenager may be easily dug up to haunt you in your adult life. Take some time to review what you have posted, and archive or delete content that no longer represents who you are today.

- Take the time to review the way online services use your private data and choose them accordingly. Always check all the privacy settings available to set the right protection for your data.

FURTHER INFORMATION

- Examples of big data being used for the benefit of society can be found on the EU Commission website: *<https://ec.europa.eu/digital-agenda/en/what-big-data-can-do-you>*.

- Information is also available about the EU regulation on the right to be forgotten: *<http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>*.

- Data & Society is an American think tank focusing on social, ethical and cultural issues arising from data-centric technological development: *<http://www.datasociety.net/>*.

- A report is available on "Civil rights, big data and our algorithmic future": *<https://bigdata.fairness.io/>*.

- The Electronic Frontier Foundation offers information on protecting your rights in the digital world: *<http://www.eff.org>*.

- The European Digital Rights also offers information on defending rights and freedoms in the digital environment: *<http://www.edri.org>*.

Since the first edition of the Internet Literacy Handbook was issued in 2003 the world of the Internet has changed tremendously. The number of Internet users has risen; users are increasingly younger, trends in how people use the Internet and what they are looking for evolve, and new pitfalls in, for example, personal security arise seemingly overnight.

This new edition takes into account the myriad changes, although the object of the Handbook still remains, namely to offer families, educators and policy-makers sufficient technical know-how to allow them to navigate, with young people, through communication technology. The new edition also expands the scope of the Fact sheets anchoring previously "new" concepts of digital citizenship and digital parenting. This edition includes 26 Fact sheets arranged under 6 thematic headings including a heading specifically dedicated to "Looking Forward" towards the future of the Internet. The Handbook is designed to be easy to use and helpful, as illustrated by the Fact sheet entitled "Finding quality information on the Web". It is also available online, where it can be downloaded either in its full format or per individual factsheet.

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It includes 47 member states, 28 of which are members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE