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?

Fact sheet 8

Social networking and social sharing

A social 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 something 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>*.