FACT SHEET 9
PRIVACY AND SECURITY

ETHICAL CONSIDERATIONS AND RISKS

Anonymity underlies many of the challenges and risks that arise from online interactions and goes hand in hand with accountability. When internet users believe that their actions cannot be traced back to them, they tend to behave in a very different way than they otherwise would. Acting ethically in seemingly anonymous situations places a much greater focus on the values of justice and fairness, which are in turn built on respect for human dignity and human rights, civic-mindedness and a responsible and respectful attitude towards oneself and others.

Privacy is a constantly evolving concept. As we embed and operationalise more and more pervasive technologies into our lives, through what is known as a normalisation process we gradually come to accept lower or different standards or values. Is it a cause for ethical concern that many young people today see George Orwell's 1984 as no more than an entertaining novel? Article 16 of the United Nations Convention on the Rights of the Child (UNCRC) underlines that children have a right to privacy, but are we breaching this right through over-pervasive technological practices, and a lack of privacy education and digital culture literacy?

Some of the latest internet-connected toys appearing on the market are raising ethical concerns among human rights advocates. Dolls, robots and other types of connected devices are capable of recording a child's innermost ideas and thoughts and, if security measures are not sufficiently strong, that information can be accessed and reused by third parties.

Families need to be more aware of the capabilities of their internet-connected household devices, what data is being collected and where this goes. Who would have thought, to give another example, that our mobile phone tracks the speed of our movements as well as informing us of how many kilometres we walk in a day, or that baby monitors are sending the very private activities that go on in the nursery through the internet. Policy makers and end users need to exert pressure on data processors to provide the option for each user to host his or her online data on his own personal cloud or even (in the case of the internet of things and connected toys, for instance) on his own local area network drive or server.

IDEAS FOR CLASSROOM WORK

Invite students to 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. Is there any information they would wish to have removed? How did it arrive online, and what is the most effective process to try to have that particular piece of content removed?

The PlayDecide role-play game on data protection and privacy (http://paneuyouth.eu/files/2013/06/PD-kit-privacy-and-data-protection.pdf) 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.

Invite students 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.

www.webwewant.eu, a website and handbook (in 12 languages) with activities created by teens for teens, contains several chapters and exercises linked to this topic. In particular, take a look at Chapter 2, "Think before you post", and Chapter 5, "My privacy and yours".

Play and learn: Being online offers 4 to 8-year-olds and their teachers and parents a range of activities on privacy and security. The publication (in 21 languages) is accompanied by an online game at www.esafetykit.net.

Resources, posters, tutorials and password generators to better design and manage strong passwords are available from the CNIL: https://www.cnil.fr/en/media.

GOOD PRACTICE/LIVING DIGITAL CITIZENSHIP

Considering privacy with a multicultural approach – Discuss privacy with your students, looking at how the concept differs across cultures and across families. Ask them to gather information to support the discussion and the reasons that may explain different notions. This activity can be linked to history or geography lessons as a means of embedding digital citizenship into these subject areas. The outcome could be a class privacy code that could be shared across the school. Revisit the code some months later to understand some of the issues children are having in applying the code in their online activities.

Creating profiles

Work with very young students to create their profile and begin by getting them to list some facts about themselves (their address, their favourite food, their parent's telephone number, etc.). After a discussion with them about privacy, have them draw a red box around private information, a green box around information that can be shared with everyone, an orange box for information that can be shared in certain circumstances, noting what these may be, for example a visit to the doctor.

With older children, explore and compare user profiles on some of the more popular social networking sites (see the Council of Europe's Internet literacy handbook, Fact sheet 8 on social networking). What private information are users inadvertently disclosing? Draw up a checklist for creating a safe user profile.

Checking cyber security – Have children bring their mobile phone to class to discover together the inbuilt and software security measures in place, but also the many "open gates" that may be allowing their information to leak. Teachers can consolidate their knowledge before conducting this exercise with students at sites such as www.tccrocks.com/blog/cell-phone-security-tips/. They could also try inviting an expert or someone from a mobile phone company to bring expert knowledge and added interest to the activity. Companies are often very interested in such opportunities to meet young users in a well-supervised context. Information on updating security measures on other internet-connected devices and research on additional tools can be found at www.epic.org/privacy/tools.html.

Get students to imagine the consequences of the loss of an online research project; how do the consequences compare with losing a computer or tablet that could be replaced? Ask them to draw up a checklist of security measures to avoid losing content, then check their list against the Internet Survival Guide (http://bit.ly/2OW3dyk). This guide, written as part of the BEE SECURE project by the Luxembourg government, provides tips, tricks and best practices.

FURTHER INFORMATION

The Council of Europe has materials relevant to this fact sheet in the Internet literacy handbook; please see ILH Fact sheet 9, "Privacy and privacy settings"; Fact sheet 19, "Cybercrime: spam, malware, fraud and security"; Fact sheet 20, "Labelling and filtering"; Fact sheet 26, "Are you the product? Big data, data mining and privacy".

Consult the Council of Europe page at www.coe.int/en/web/internet-users-rights/privacy-and-data -protection to learn more about its work in the field of data protection. Fact sheet 19 of the Council of Europe's Internet literacy handbook is dedicated to cyber security and related topics. It may also be useful to read about the General Data Protection Regulation implemented in EU member states in May 2018: https://gdpr-info.eu/.

Data protection authorities, highly specialised in the domain of privacy and security, play an important role in assisting educators in the digital education of citizens. They recently developed a training framework for students specifically dedicated to data protection, for use in a cross-curricular approach in official school programmes and training courses for educators: the "Personal Data Protection Competency Framework for School Students" (https://bit.ly/3mAFfwY).

In early 2018, the UK Council for Child Internet Safety (UKCCIS) published a framework to equip children and young people for digital life. "Education for a Connected World" aims to identify the skills and competences that children and young people need to have at different ages and stages to be able to navigate the online world safely and responsibly. It interestingly focuses specifically on eight different aspects of online safety education, including self-image and identity, managing online information, and privacy and security (http://bit.ly/2P2ildz).

The American online safety organisation "iKeepSafe" has developed an extensive privacy curriculum providing classroom and family activities for tweens and teens (https://ikeepsafe.org/privacy-curriculum-matrix/).

How to Geek offers concrete, well-explained ideas about creating a password (www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/). Other security-related activities for older children have been published by a British organisation specialising in STEM (science, technology, engineering and maths): (www.stem.org.uk/resources/community/collection/401587/gcse-cyber-security).

The European Handbook for Teaching Privacy and Data Collection at Schools (Gonzàlez Fuster G. and Kloza D. (eds), 2016), provides lesson plans adapted for younger and older students, a mini-bill of privacy and data protection rights, glossary and resource list (http://arcades-project.eu/images/pdf/arcades_teaching_handbook_final_EN.pdf).