ARCADES

Introducing d**A**ta p**R**ote**C**tion **A**n**D** privacy issu**E**s at school**S** in the European Union

http://www.arcades-project.eu/

CALL: JUST/2013/FRC/AG
AGREEMENT NUMBER: JUST/2013/FRAC/AG/6132

Workstream 1: Preparing the two-day seminar for teachers.

Deliverable 1.2: The European Handbook for Teaching Privacy and Data Protection at Schools – the set of materials for teachers.

Prepared for the European Commission
Directorate General Justice
Co-funding by the European Union under Fundamental Rights & Citizenship Programme

Brussels, September 2015

LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES Vrije Universiteit Brussel

INFORMATION COMMISSIONER

GIODO Generalny Inspektor Ochrony Danych Osobowych

National Authority for Data Protection and Freedom of Information

The European Handbook for
Teaching Privacy and Data Protection at Schools
– the set of materials for teachers.

Responsible partner: Law, Science, Technology and Society (LSTS), Vrije Universiteit Brussel (VUB)

Editor: Gloria González Fuster (VUB)

Author	*Institution*	*E-mail address*
Jelena Burnik	IPRS	Jelena.Burnik@ip-rs.si
Polona Tepina		Polona.Tepina@ip-rs.si
Viktor Árvay	NAIH	privacy@naih.hu
Laura Kozma		
Kata Nagy		
Zsófia Szántó		
Julia Sziklay		
Zsófia Tordai		
Piotr Drobek	GIODO	p_drobek@giodo.gov.pl
Urszula Góral		u_goral@giodo.gov.pl
Paweł Makowski		p_makowski@giodo.gov.pl
Marta Mikołajczyk		m_mikolajczyk@giodo.gov.pl
Paul De Hert	VUB	paul.de.hert@vub.ac.be
Gloria González Fuster		Gloria.Gonzalez.Fuster@vub.ac.be
Dariusz Kloza		Dariusz.Kloza@vub.ac.be

Delivery date: 5 October 2015

Status: Version to be submitted to the European Commission.

Table of Contents

Presentation

This handbook has been prepared in the context of the Introducing Data Protection and Privacy Issues at Schools in the European Union (ARCADES) project, co-financed by European Union's (EU) Fundamental Rights and Citizenship Programme, managed by the Directorate-General for Justice at the European Commission. It is the outcome of a joint effort by all project's partners – the Polish Bureau of the Inspector General for Personal Data Protection (GIODO), the Information Commissioner of the Republic of Slovenia, the Hungarian National Authority for Data Protection and Freedom of Information, and the Law, Science, Technology and Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB) –, under the coordination of the latter.

It aims to provide a useful tool for teachers of any EU school wishing to educate children and teenagers about privacy and personal data protection. Its ambition is to be of direct use all across the EU, and thus it focuses on providing essential knowledge that is valid and relevant among all EU Member States, based on relevant legal instruments applicable across Europe, and most notably the EU Charter of Fundamental Rights. For additional legal information, teachers should refer to the national data protection authority of their own country.

The handbook is written in clear and simple language that will help teachers find the right words to explain to their pupils the issues at stake. It is structured in ten chapters covering different facets of privacy and personal data protection, all of special relevance for children and teenagers. Each chapter advances a set of key ideas and puts forward subjects for discussion, recommended activities or concrete tips, depending on the subject. When appropriate, chapters include also 'real life' cases or examples. Additionally, the final sections of each chapter highlight ideas that could be especially important for younger children, and those that could be of special interest for older or more advanced pupils. The key terms using in the different chapters are defined in a final glossary.

Teachers are encouraged to familiarise themselves with the whole handbook, and to freely use the different elements of the chapters in accordance with the needs of their class. They are also warmly invited to share their experiences in teaching about privacy and personal data protection with the authors of the handbook, to contribute to the sustained improvement of this tool.

1. Introducing privacy

What is privacy? And why is it important?

Objectives

This introductory chapter should help pupils to:

- Learn about privacy.
- Shape a reflective attitude towards it.
- Understand the importance of privacy both offline and online.

Key issues

Privacy is about protecting what is **private**, but also about the possibility '**to be yourself**' and to have the chance to live in accordance with your own preferences, shaping your life in line with your own will. **Privacy** is thus about shielding yourself from the gaze of the others, but also about being able to reject interferences with your private sphere by others – be it the State, parents, friends, teachers or strangers.

Privacy has always played a pivotal role in the functioning of **modern democracies**, and has thus been recognised as a **human right**. Its legal recognition became especially prominent after the Second World War as a reaction against totalitarian regimes. Its value is acknowledged in all European legal systems, typically as a **fundamental right**, as well as internationally. States shall not interfere with the right to privacy, but they must also ensure that this right is protected from attacks by others, like private companies.

The **Charter of Fundamental Rights of the European Union** enshrines the right to respect for private life in its Article 7.

The value of privacy has also been recognised by psychologists, who suggest there is a '**restricted privacy**' and an '**open privacy'**. 'Restricted privacy' would be about keeping things secret, preserving the intimacy of the body, of emotions, or feelings, whereas 'open privacy' would be about being able to express oneself **in public**. Both types of privacy are necessary, notably to maintaining our sense of self-worth and to protect our image in the society and social relationships.

Childhood is a unique period in each human being's life, during which the protection of privacy is particularly important. **All children**, regardless of where they live, have the right to life and development, to grow up in an environment that respects freedom and dignity, to **privacy** and to **personal data protection**.

New technologies raise special challenges for the protection of privacy. We increasingly communicate, work, study, have fun using technology… we actually increasingly **live with and through technology**. Everybody – also children – should be able to enjoy their privacy rights always, that is, also when they are **online** or connected.

Definitions

Right to privacy

Real life cases

Famous people are particularly vulnerable to privacy violations. The media know that publishing some funny or unexpected pictures about them could attract many curious people. The photographers known as '**paparazzi**' can spend many hours trying to catch images of celebrities. Even famous people, however, have a right to privacy, and thus the media should not publish pictures of them that do not have a particular public interest (for instance, because they are just going about their daily life) or if they reveal something very private that the celebrity would prefer to keep private (for instance, if they went to the hospital for a health check). Many famous people have been fighting the publication of pictures about them in the press – including actors, fashion models, and princesses.

Ideas for discussion

Pupils can be asked to discuss these questions:

1. ***Personal experiences***: Have you ever had your privacy violated? What happened? How did you react?

2. ***Shaping a reflexive attitude****:* Can you imagine a society where there would be no privacy at all? Would you like to live there? Can you imagine any problems that would emerge? Try to think of special categories of people with special privacy needs: people with health problems they do not want to share publicly, journalists wishing to carry out investigations in private, teachers who wish to keep some distance from their pupils, people who want to be politically engaged that do not want to be scrutinised by their opponents, etc.

Recommended activities

1. This exercise can help pupils think about what constitutes their privacy, how we might need more 'privacy' in some contexts than in others, and how does it feel to have your privacy invaded:

    - Everybody in the classroom should greet each other, as if they had not seen each other for a few months. **Observe** the different ways of greeting, and **discuss** these questions: Do close friends greet each other in the same way as not so close friends? Would you greet a member of your family differently? How do strangers greet? And how would you feel if a stranger wished to greet you too effusively?

2. To explore the many dimensions of privacy, write on the board the word 'privacy' and invite pupils to **draw a mind map** of related terms: first, write down any words connected to privacy; second, try to create group of words that seem to relate to different dimensions of privacy (for instance, privacy of the body, privacy of communications, etc.).

For the youngest

Young children should learn that privacy is about keeping things for oneself, but also about having space to be themselves. They should know that people **should respect their privacy**, and that they should **respect other people's privacy** too.

For the most advanced

Most advanced pupils should understand that the right to privacy is a **fundamental right** that plays a crucial role in the functioning of democratic societies. It marks the limits of the State intervention in the lives of individuals, and thus helps us to live in freedom.

2. Introducing personal data protection

What is personal data? And what does it mean to have a right to the protection of personal data?

Objectives

This chapter will help pupils to:

- Learn about the meaning of **personal data protection**.
- Know what is exactly '**personal data'**, and why it should be protected.
- Learn about '**sensitive data'**, or data deserving special protection.
- Increase their awareness of their **rights** as data subjects.

Key issues

In addition to ensuring the right to privacy, the law also grants individuals a **right to the protection of their personal data**. This right is recognised as a fundamental right in modern societies because of the dramatic effects misuse of personal data can have on the life of individuals: for instance, when some data are linked to the wrong person, or when an organisation gains too much knowledge about some people.

The first laws on personal data protection saw the light in the **1970s**, when governments and companies started using computers to store and process information on individuals. There were fears that with the machines gave those who had information more and more power over individuals, who had less and less control on what happened to their information. Nowadays, the processing of personal data is more widespread than anyone had imagined, making the right to personal data protection even more necessary.

The **Charter of Fundamental Rights of the European Union** enshrines the right to the protection of personal data in Article 8.

The law protects through this right all '**personal data**', which is any data, digital or not, that can be **traced back to a particular person**. It might be a piece of written information, a picture, a video, or even a sound recording. It could be a telephone number, an email account, or somebody's shopping list, as long as these can be linked to a specific individual. Even if the data look uninteresting or irrelevant at first sight, they will be considered personal data that deserve protecttion. The sum of different apparently uninteresting data could indeed reveal many interesting things about a person, and thus the law protects all personal data in general.

There are, however, some types of data that are particularly **sensitive**, and thus are especially protected by the law. We consider sensitive data, for instance, the data that refers to peoples' political or religious **beliefs**, their **health**, their **ethnic origin** or their **sex life**. They are granted reinforced protection to avoid people being discriminated on the basis of any of these issues, and to prevent any stigmatisation, but also to allow people to keep these matters as private as they wish.

To prevent the misuse of personal data, the law gives **a series of rights** to any individual whose personal data is processed by somebody, imposes **obligations** on those who wish to gather or further use other people's personal data, and foresees that an **independent data protection authority** shall monitor that all these rules are respected.

Individuals whose data is processed are called '**data subjects'**. We, as data subjects, all have the right to:

- be informed about **who** uses data about us, **which data** they use, and **for which purpose** ('right to be informed');
- **ask** those who use our data to tell us exactly which data they have about us ('right of access');
- require the **correction** of any wrong data ('right to rectify');
- require the **erasure** of data when those who use it have no valid reason to do so ('right to object');
- **refuse** or **consent** to some uses of our data;
- **complain** to an independent authority if our rights are not respected; and
- claim protection of our right before a **court.**

Definitions

Data subject

Personal data

Right to the protection of personal data

Sensitive data

Real life case

In 2007, an Austrian university student, Max Schrems, was studying the laws on privacy and personal data protection and decided to test his 'right of access': he had a profile on Facebook, so he contacted it and asked for a copy of all the data Facebook had about him. As he had only been using Facebook for a few years, and not very often, he was very surprised when, in answer to his request, they sent him more than 1.200 pages of information about him. He was even more surprised when, reading all the information, he discovered that Facebook kept pictures that he thought had been deleted, as well as other data that he believed they should not have. Since then, Schrems has initiated a European-wide initiative putting pressure on Facebook to respect all their obligations, notably by taking them to court.

Ideas for discussion

1. ***Thinking about the problem.*** Personal data protection applies whenever people collect personal data, even if they just want to collect the data, store them, and promise never to use them at all. Pupils should be invited to think about why is this so: Why could it be a problem that an organisation or company starts collecting plenty of data

about everybody? Do you think it should be allowed for them to collect data about you without you knowing?

Recommended activities

1. ***Recognising personal data.*** The protection of personal data applies to all personal data, but it is not always easy to know if data are 'personal data' or not. As a matter of fact, data could not be 'personal data' at a certain moment, and become 'personal data' afterwards. To understand better these issues, pupils should **look at a picture** of somebody whose face they cannot seen, and discuss whether they think it is personal data or not. They should consider then what would happen if somebody tagged online the picture with the name of the person: Would it be personal data?

For the youngest

Youngest pupils should be made aware that whenever somebody wants to have data about them, they have some **rights** on that data.

For the most advanced

Advanced pupils should know how to recognise what is personal data, and have a clear view of their **rights** upon such data: to know who has them and why, to access them, to rectify them and sometimes to have the data deleted.

3. Who wants your personal data?

Why is the protection of personal data so important nowadays? Who is interested in getting our data, and which obligations must they respect?

Objectives

This chapter aims to allow pupils to:

- Get a picture of why organisations collect, store and use our personal data.
- Learn about the obligations they have when they use the data.

Key issues

Nowadays, **we all produce huge amounts of personal data** on a daily basis. We create personal data when we are **online**, sometimes because we post information, pictures, or videos about people or share them with others, or simply by checking our emails, reading online news, playing online games – because these activities generate data that might be linked to us. We also create personal data **offline**, when we make a phone call, when we shop and pay with a bank card, when we use public transport, or even just when walking by – if our image is caught by a CCTV camera. In reality, an increasing share of our **offline** activities often have an **online dimension**: when we go to the cinema, to a concert or to a football match we might buy the tickets online, also generating more data.

Generally speaking, companies and organisations collect, store and use our personal data to deliver a specific service and deliver it the best way they can. Often they will pursue a **highly important objective**, like providing childcare or medical treatment.

Some companies, however, like to collect **as much data as possible** about people in general and about their costumers in particular basically for what is known as **'marketing purposes'**. This allows them to refine the way they work and increase the number of costumers or make them spend more money for their services.

Personal data can thus have a considerable **economic value**. For many companies, personal data are an object of desire and a source of considerable revenue: some of them use personal data for advertising and making or increasing their profit. Personal data can also be of **great interest** for **public authorities**, as they can allow them to gain new insights on individuals or groups of individuals.

The uncontrolled use of personal data, however, could grant private companies and public authorities excessive power, leaving individuals in a delicate position.

To prevent the misuse of personal data, the law imposes a series of obligations on those who wish to process it. Known as 'data controllers' they have the obligation to:

- process personal data **fairly**;
- process personal data only for a concrete, **specified purpose**;
- use as little data as possible (that is, use only data that is adequate, relevant and not excessive) and store it **only as long as this is necessary;**

- keep the data **accurate**, **complete** and **up-to-date**, ensuring their quality; and
- keep the data **safe** and **secure,** preventing access to anyone who does not have the right to lay hands on it.

Definitions

Data controllers

Ideas for discussion

1. ***Data breaches:*** Pupils should think about the importance of imposing a series of obligations on companies and organisations that use huge amounts of personal data by reflecting on data breaches, that is, the cases when a wrong person gets access. They should consider questions such as: Have you ever heard of any case of 'data breach', or companies or organisations losing control on the data about some people? Would you be worried if somebody that has information about you had suffered an attack by hackers who could steal your data? Which kind of 'data breaches' would worry you the most? Why?

Recommended activities

1. ***Loyal clients.*** Many supermarkets and commercial chains encourage their clients to have loyalty cards that they have to or may show every time they shop. This exercise aims to start a reflection in the class about the loyalty schemes and the processing of personal data that they entail.

- First, pupils should **talk about** their perception of loyalty cards: Do you think they are useful for clients? Do you think they are useful for companies? What kind of information do they think companies collect through these cards?

- Second, each pupil should **pick up** a loyalty card that they or their family uses, and provide a short description of: 1) the information that one has to give the company to obtain a card; 2) the information that the company collects when they use the card, and 3) the purpose of this data collection according to the company. This might require checking up the company's website or a brochure, or asking them.

- If there happen to be pupils whose family does not use any loyalty card, they can, as **an alternative**, describe the information that shops collect about them when they shop, if any. For instance: they shop online, do companies register information about their shopping activities?

- **Share** and **compare** the results of individual explorations.

- **Discuss** what can be the advantage for companies to collect information about their clients.

- Finally, **reflect** about what has been learnt through the exercise: Were pupils aware about the data that was collected about them and their family? Do you think people are generally fully aware of what is happening with their personal data? Would it be useful for them to be better informed?

For the youngest

Youngest children should learn that the data about them are **precious**, that people should only collect data about them if they have a good reason, and that they can only do it very carefully.

For the most advanced

The most advanced pupils should be made aware of the **vast quantity** of personal data that we generate daily, and of the **variety** of companies and organisations interested in using them, for many purposes. They should also learn that whenever somebody processes personal data protection, some **obligations** must be respected in order to protect us.

4. Decide wisely, and remember to let people decide too

We all have a say when somebody wants to collect or use our personal data. This means that people should take into account our wishes with regard to what happens to our personal data and that we should do the same when it comes to other people's data.

Objectives

This chapter shall help pupils to:

- Learn about the possibility to **refuse** or **consent** to the collection of some personal data.
- Be aware that consent can be **revoked.**
- Understand that sometimes they might need to ask for **other people's consent** before they share content online.

Key issues

Sometimes we are **obliged** to give some personal data about us to other people. If we want to have a pizza delivered home, we surely need to give our address to the pizza company – otherwise they wouldn't know where to deliver it.

In some cases, however, companies would like to collect **more data than strictly necessary.** They might wish to know some additional data about their costumers or the users of their services, like their age, gender, or favourite hobby. They may ask for these data, but they need to tell what they plan to do with it, and should give people the possibility to **refuse** or to **consent.**

To be valid, the consent of the person needs to be **freely given**, **specific**, **informed** and **unambiguous**. This means that:

- we cannot be forced to 'consent' to give our data;
- people can only ask us to consent to specific data uses, and not generally to whatever purposes they might think of;
- people can only ask us to consent if they give us detailed information about we are consenting to; and
- people can only say we gave our consent if we express this clearly.

Before deciding whether to accept or refuse a request for consent, individuals should take the time to understand **which data** will be collected, **for what purpose**, who will be **responsible** for keeping it safe, and **how to contact them** if they change their mind and prefer the data to be deleted. If all this is not clear, or if they are not comfortable with any of this, individuals should **not consent**.

As it can be difficult for **children** to understand the consequences of giving personal data away, the law says **they cannot be asked to consent** before they reach a certain age. Therefore, if a company or organisation wants to ask children who are not old enough to consent by themselves for personal data, they should **ask their parents**

(or guardian), who will then refuse or consent. This does not mean that the adults do not have to take into account the children's' views on all this, which they should actually take into consideration as much as possible. Indeed, children have a right to **express their views** in all matters that affect them.

Even when somebody has consented to give away personal data about them, they remain **free to change their minds**. This is particularly important in relation to data that might let other people know where individuals are, known as **'location data'**. It could be that a person accepted to have her mobile phone located by an application to search for an address, but then wishes to move around untracked by others. It is her right, so it is her right to revoke the consent. Devices that give information about where they are should actually regularly remind people about it: it could be they forgot they had given consent, or that consent had been given by another person using the device.

Everybody who is in a position to give consent has also the right to **revoke the consent**. Additionally, when parents gave consent on behalf of their child, but the child has grown up and, having obtained the capacity to consent, prefers to revoke such 'parental consent', they can also do it.

Finally, it is important to know that we can infringe **other people's rights** if we don't ask them if they consent to us sharing some data about them. When we wish to post online a picture with other people, we need their authorisation. We should ask them if they agree with the idea, and **respect their decision** if they tell us they prefer not to have the picture online. If the person is a minor, we should ask the parents or a guardian.

Definitions

Consent

Ideas for discussion

1. ***Freely given:*** In principle, we are only able to 'consent' to some data processing practices when we are completely free to say no. Sometimes, however, those who ask us for our consent seem to be in a special position, for instance because they are very popular, and it is not that easy to refuse. Pupils should think whether they feel really 'free' to use or stop using the online services and applications that they use regularly (and which collect personal data about them), like social networking platforms. Consider questions such as: Why do you actually use a specific service and not another? Is it because most of the people you know use it too? Do you feel pressure to use a service because of this?

Recommended activities

1. ***Which terms and conditions:*** This exercise is aimed at pupils who are mature enough to actually consent to data processing practices. It aims to illustrate that sometimes we express our 'consent' without taking the time to be properly informed about what we are consenting to.

- Pupils should, first, **write down the name** of an application or online service that collects personal data and that they use particularly often. They should ideally not all chose the same, but at least a few different services.

- Second, they should write down **anything that they remember** from the 'terms and conditions' or 'privacy policy' of that service, which are supposed to explain what does the company do with their data, and that they had certainly to accept in order to register. If they do not remember much, they should at least try to remember if they came across 'terms and conditions' or a 'privacy policy' at all.

- Afterwards, they should **compare** their answers with reality, by checking the service or app and their real 'terms and conditions' or 'privacy policy'.

- Finally, the class should discuss what can be learnt from this experience: Do pupils actually know much about what the companies tell them? Did they really take the time to read? If yes, do they think everything was well explained?

For the youngest

Youngest pupils should know that they **should never give away data about them** without the permission of their parents. Also, they should understand that they cannot post information about other people (including sharing pictures or videos) without asking them first.

For the most advanced

The most advanced pupils should acquire the **skills necessary to give (or refuse) consent**: when somebody asks them for their personal data, they should make sure they understand what is the purpose, which data will be taken, who will keep them, and how to contact them if they want more information or their change their minds. They should always feel free to say no, and question anything they did not understand. Equally, before using **personal data about other people**, they should **ask them** – and respect their choices.

5. Digital identity

How to grow up with a digital identity? Online information about us can have serious implications in our life so it is important to ask ourselves what should we share, when and under what circumstances.

Objectives

This chapter shall help pupils to:

- Become aware of their online presence, and adopt a more reflexive attitude towards disclosing information online.
- Think about the importance of people's **digital identity**.
- Reflect about how to control their digital footprints.

Key issues

The combination of all online information about us defines what can be called our '**digital identity'** or 'online presence'. This is the picture of us that somebody could get if they did not know us at all, but knew our name, just by making a search with an online search service. It can be seen as an element of our '**identity**', which has many dimensions: we are not exactly the same person in the eyes of our grandmother as in the eyes of our best friend, we do not behave exactly in the same way in our room and in a shop, we might not have the same reputation at school and where we spend the summer holidays.

As people increasingly use the Internet, **'digital identities'** and **'online reputation'** have become very important. When somebody looks for a job or applies for a scholarship, potential employers and funders could have a quick look online, to get some complementary info about the candidate, and, if they find something they dislike, not hire or give them the scholarship. If one day you meet somebody you would like to be your friend, or your partner, it could be that this person checks up the Internet to know more about you.

Our 'digital identity' is never exactly the same as our real identity. In some cases, our 'digital identity' is particularly **misleading**, and makes people believe that we have done things we never did, or keeps reminding everyone of something that we consider is a thing of the past.

Europe has now recognised a '**right to be forgotten'**, which allows individuals to request search engines not to show, when people look their names up, any results that are **inadequate, irrelevant, or no longer relevant.** The existence of this right reminds us that the results that people see when they look us up can have a real impact on our lives.

This right, however, does not mean that one can ask for the removal of any personal information that is online. Actually, even when we do have the right to have some information removed, it could be that **in practice it is not easy** to get any data off the Internet. Or it could be that when it is removed other people have already copied them on their devices, and spread it around.

The best thing to do is, thus, to **think twice** before we post any information or media online. Minors should be aware that all data about them are like 'digital breadcrumbs' or '**digital footprints'** that could one day be **traced back to them**, and that are **difficult to erase**. Some are actually so difficult to erase that it might be better to think about them as '**digital tattoos'** that could threaten to stay with you forever.

Definitions

Digital identity

Real life cases

- A Spanish man was once caught urinating in public and sanctioned for that. In accordance with Spanish law, as the police did not know where to send the fine, they made a public announcement in an official journal, which was also published electronically and made accessible through search engines. The man eventually started to work as the headmaster of a school. A pupil made a search using the headmaster's name, discovered the sanction and shared this with all pupils. This seriously affected the image they had of their headmaster, rendering his job very difficult.

- A Hungarian student had made some pictures during a history lesson at his University, where one could clearly see his face and some Nazi symbols. These pictures where published online, and when people searched for the student's name on the Internet, they automatically appeared. He was worried that this could affect his chances to get a job, so he asked the search engine to stop linking the pictures to searches made using his name. With the help of the data protection authority, he managed to obtain this.

Tips

There is something online about you that you would prefer to get rid off?

- First, contact the person who published it, and ask them to delete it.
- If it was you who posted it, try to delete it yourself. All online services should have a way to get rid of you whole profile or account, if you wish.
- If that does not work, contact the person or the company who owns the website or the platform.
- If that still does not work, ask an adult to help you. You can also contact your data protection authority for guidance or help.

Ideas for discussion

1. ***Why should online reputation matter?*** Pupils should think about which when and why could their online identity matter. This can notably be done by:

- Thinking about **typical situations** where people may check out online information about other people. For instance: related to work (Would you do an

online search on somebody before offering them a contract to work in your company?), housing (Would you do an online search on somebody before sharing with them an apartment?), social relations (Do you think it is possible that people you meet in the future will be tempted to know more about you by checking the internet?), etc.

- Thinking about **special categories of people** for which online reputation can be very important. Pupils could discuss what would happen if any of them was to have a career in politics, or become a famous actor, or a famous sportsperson: Would there be a special interest in online information about them? Would then they prefer to have some pictures or data about them offline?

2. ***What feels totally wrong online?*** Pupils should think about which data can be especially problematic when publicly available online. To do so, they can reflect on their personal experiences, and try to remember if they have ever seen something that gave them a really bad impression about somebody. Think, for instance:

- About data that could be **too intimate:** Are there things it could be wiser never to share online? What? Why?

- About data that could be **misunderstood:** Are there things that could be too easily taken out of context? Are there pictures that are ambiguous and could lead to wrong interpretations? Are there profiles that give a too partial account of who you are?

- About data that could become **rapidly obsolete**: Are there things that look cool today but might be completely out of fashion tomorrow? Have you ever felt ashamed about something you had done a few years ago?

Recommended activities

1. Pupils should be encouraged to **explore** which **information about them** is available online. In some cases, this could lead them to unexpected discoveries, like seeing that some information that they thought was private is actually available to the general public, or to the realisation that what they believed was only accessible to their (online) friends is actually also accessible to anybody. To avoid any unpleasant situations for the pupils, they should be able to do their exercise on their own – possibly at home. They could be invited, afterwards, to **reflect in writing** and/or **discuss** in the class on what they have learnt through this experience.

2. Another enriching exercise is for pupils to **look up** for **information about other people**, especially if they are people somehow related to them:

- They could, for instance, be separated in different groups and given a limited time to gather as much data as possible about **their teacher**. Before doing this exercise, it is strongly recommended that teachers carry out an extensive investigation of the online information available about them, to avoid bad surprises. When the time is over, the groups will compare the information obtained, and discuss these questions: Have you learnt something you did not know about your teacher? Is there any information that you think your teacher should try to get off the Internet? Why?

- Another possibility is to ask pupils to see if they can find, through the Internet, people who have **the same as theirs**. Some of these cases will be selected, and small groups of people will gather publicly available information about the homonymic person. Each group will then present a description of that person as they can imagine it using the information available online. In light of their experience, they shall discuss these questions: Can you obtain a detailed image of people just by doing an online search? What could happen if somebody was looking about one of the pupils in the class that has the same name as other people?

For the youngest

Youngest children should realise that anything that is online could be seen by many different people, and that the different pieces of information about us that are online give people a certain image of us, so we need to think twice about what to put there.

For the most advanced

The most advanced pupils should understand that online information could have serious implications for their lives, so it deserves all of their attention. As a basic rule, they should avoid publishing online any information they would not be comfortable sharing with a wide audience.

6. Online targeting

Being connected is not only about actively posting and sharing information that we chose: whenever we use electronic devices, they could be producing and sending away data about us and about what we are doing. These data are particularly valuable for companies that sell advertisement space, which often collect our data while offering 'free' services.

Objectives

This chapter shall help pupils to:

- Realize that their online activities are often monitored.
- Learn that companies show them ads and products on the basis of their previous behaviour.

Key issues

Whenever we use computers, mobiles, iPads, game consoles or any device to communicate or connect to the Internet, we are **generating data**. Some of this data is **about what we are doing**: the websites we visit, the videos we watch, the games we play, the people with whom we exchange messages, or the searches we make, as well as many other types of data. Some of the data is **about where we are**: this data is used to locate us on a map, or to connect us to a local version of a website, for instance. Finally, some of the data is **about us** (our phone number, our email account, all our identifiers): it allows companies to link up all this information and build a quite detailed picture of **who we are**, the kind of life we live, **what we like** and **how we could spend our money**. As a matter of fact, they might also have a pretty accurate idea of how much money we have. Companies and other organizations, indeed, use all of this information to '**profile'** people, placing them in different categories.

We are not always **aware** of all this data collection, even if, in principle, whoever collects our data and uses it should tell us about it clearly. In practice, people tend to accept all sorts of '**terms and conditions'** before using an Internet service or downloading an application without even reading them. When they read them, they might not really understand them – which most probably is the case if they are minors.

Likewise, nowadays websites that collect personal data using what is known as '**cookies**' have to inform the public about which data is being gathered and for what purpose, allowing them to accept or refuse. Most people, however, do not have time to think about the cookies of each website, or have trouble understanding what is actually at stake.

Most of the time, companies will actually profile people based on their online behaviour in order to **sell advertisement space**. If a website is often visited by children, they will try to sell advertisement space on it to toy companies, arguing that they are the best public for it. As a matter of fact, companies are also able **to adapt the content of each ad to what they think is of interest for each user.** When children that seem to like puzzles visit the website, they will be shown ads for puzzles.

These practices are called '**behavioural advertising'** or **'targeting'.** Minors should be aware of the fact that online content is sometimes targeting them on the basis of their previous behaviour: the links they see when doing an online search are partially determined by data gathered about them, as well as by the products that are given special relevance in some online shops.

Minors should, in general, know that many companies that seem to be offering their services '**for free'** are actually not asking for money from their users because they **make money** thanks to the data they collect about them. As the more people they attract, the more money they will probably make, it is convenient for them to let people use their services 'for free'.

Definitions

Behavioural advertising

Profiling

Ideas for discussion

1. ***Could little bears spy on children?*** Some companies, including toy companies, are developing 'smart toys' that would interact with their owners and send to the company information about the children. The information is, in principle, supposed to make the reactions of the toys more realistic and interesting, but it could also be used by the companies to gather extra data about children. Pupils should discuss whether it seems to them a good idea that children have bears or dolls with cameras and microphones that can record sounds and images and send them to a company. Would they like to have one? If so, do they think they should be able to turn them off? What if they forget to turn them off, and the toy registers things they would not like a company to know?

2. ***Equal chances?*** When we are online, some of the content we see depends on what some companies think we are interested in, or would like to buy, on the basis of the information they have about us (and their interpretation of it). This could mean, for instance, that pupils from the same class are shown different ads when they visit the same website. Sometimes, the content of the ads displayed might not be particularly important or life changing – some pupils could be shown ads for some clothes, and others for another type of clothes. It could be, however, that the differences are actually about things that matter more: you could see ads for a travel that the others do not see, ads for different school or university programmes, ads for different scholarship opportunities, or even different jobs. Pupils should discuss whether they see this as being fair, think of cases where it could be a problem, and talk about possible ways to deal with it.

Recommended activities

1. ***Anonymous information?*** The following exercise is an invitation to think about the information that can be derived from our activities and preferences.

- Each pupil should choose a **fictional name** that should cover up their identity, and write on a paper, under their fictional name, a series of pieces of **information** to be determined by the teacher depending on the pupils' age. They can include: favourite TV programmes, favourite clothes, favourite sports, languages spoken, favourite music, recently watched film, recently read book, etc. During this first stage, the teacher should not explain the purpose of the game.

- All pages should then be mixed. The teacher should pick up randomly a page and start reading it aloud. The author should do their best to conceal their identity, not to be unmasked. All other pupils must **try to guess** who is the author: Can they guess it with one piece of information? Maybe with two? Maybe with three?

- Afterwards, or in case nobody could guess who the author was, they should all think about **who could be interested** in contacting a person with that kind of a profile: would that data have a commercial value even for somebody that does not know who is the author?

- The exercise can be **repeated** with different pages/profiles.

- Finally, advanced pupils can be asked to think about how could companies get **online** information as the one provided by the pupils: Does somebody keep track of the things we search for? Does somebody ask us to express what we 'like'? Does somebody have information on products we have been checking? Does somebody have information on the videos we like to watch? And so on.

For the youngest

Youngest children should be told that many of the electronic devices they use (or could use soon, maybe) are connected and **generate data about their lives**: mobile phones, computers, tablets, game consoles,… Through all of these machines, companies try to get information about what we are doing to be able to sell us their products and services.

For the most advanced

The most advanced pupils should get an understanding of how their activities can be tracked through the different devices they use, and realise that some of the information they see online, like ads, might not be the same as what other people see.

7. Keeping secrets really secret

Making sure that our data are protected starts with us. To keep our data safe, we must behave carefully, and take some basic technical precautions.

Objectives

This chapter shall help pupils to:

- Be aware of the threats that could put their data in danger.
- Learn how to better protect their personal data.
- Learn about '**privacy settings'**.
- Be aware of **'identity theft'** and '**phishing**'.

Key issues

We keep our **digital data** in many different places. Some of it is in physical things we have, like computers, or tablets, or smartphones. Some of it is actually stored by other people, and we might reach it by logging into an account or profile. It is important that we take all the necessary measures to make sure that our **data is secure**.

We should thus make sure that we protect our devices, for instance by locking them and accessing them with a code. This can prevent access by people

We also need to make sure that we protect our online profiles and accounts. As most of them can be accessed using a password, it is crucial that we have **strong passwords** and that we keep them **strictly to us**.

Keeping our passwords for our personal accounts and profiles secret means keeping them **seriously and strictly to us**, and **not sharing them with anybody**; not even with our best friends, or with the love of our lives. Keeping our own passwords safe is **our responsibility** and we cannot share this with anybody.

Pupils should know that if anybody asks them to disclose to them their personal passwords as a proof of their friendship or of their love, they should not accept this, because it could put in danger their data and the data of all their contacts. As a matter of fact, the person who asks should, as a proof of their friendship or love, fully respect their privacy and **stop asking**.

Online, we need to make sure we are always in control of what happens to our data by mastering the '**privacy settings'** of the services we use. Privacy settings are mechanisms that allow the users of services to decide (to a certain extent) who will be able to access their profile information as well as any other content they might share.

Even if 'privacy settings' are called as such, and although they are supposed to help users in control of their data, sometimes it is **not easy** to use them: they could be, for instance, different settings to adapt to control the information of a profile, to decide what happens to posts, to chose who will see comments to other people's posts, etc.

It is important that minors:

- do not share publicly any information such as their address, phone number or email account;
- have a clear view of which of the information they post, upload or share will be available to everybody, which will be only available only to a few people, and who are these people;
- know which information can be found when somebody searches for their name or alias.

Keeping our data safe also requires paying attention to the emails we receive. Some of the messages we get may actually be a **fraud**, or a scam. For instance, you might receive an e-mail telling you that you have won an award, or inherited a fortune from somebody you had never heard about. To access the invented award or the inexistent money, they will ask you for some personal information that they will actually use to take money from you.

A particularly dangerous practice is what is known as '**phishing**', whereby people are made to believe that a company wants to have access to some of their **confidential data**. It could a message that **looks like** it is sent from a bank, or an email provider, or the company allowing you to buy online games and applications…

They will tell you they absolutely need you to provide your password or any other data such as your date of birth, telephone number or address, and then use this information to access your online accounts and make if as they were you, in what is known as '**identity theft'**. With only a few credentials mischievous people could even try to use your money (or your parents' money).

Minors, therefore, need to be **very cautious** when they receive emails like that and **never give any confidential information** even if the messages sound alarming or urgent.

Definitions

Identity theft

Phishing

Tips

- Lock your devices so you are the only one that can unlock them, for instance with a password.

- By checking the history of your web browsing, people could see which websites you have been visiting. When you do not want this to happen, remember to ask the browser to stop remembering, or to delete what was already registered (normally, through the 'tools' menu).

- When you install an app on your phone, check which information it wants to access.

- When you receive 'spam' (unsolicited emails), do not open the attachment – just ignore it. It might contain links to malicious software.

- Create **strong passwords** in a way that will allow you to remember them:
  - Do not use as your password data about you such as your birthdate.
  - Do not keep your password near your computer, phone or tablet.
  - Try to use long passwords with a variety of types of characters: include small and capital letters, numbers, signs.
  - Avoid just typing characters because they are close to each other in the keyboard.
  - You can easily remember a password if it comes from a sentence, such as: I Like Strong Passwords and Protecting Privacy: ILSPP.
  - Remember to log off when you use public computers or shared devices.
  - Change your password every now and then, just in case.

- If you receive an email asking you for data, it could be a scam. Take the time the read it carefully, check all the details and, when you can, look up the Internet to see if somebody has already received a similar message, for instance by searching for one of the sentences used in the email with a search engine. Remember you should **never give your passwords** through email. Serious companies will never ask for confidential information to be sent by email: if you receive an email that looks like they are asking for that, it is most probably a **phishing** attempt.

Recommended activities

1. ***Set your privacy***. This exercise aims to help pupils realise the importance of paying attention to the 'privacy settings' of the online services or applications they use. Pupils should:

- First, **chose** an online service or application that they use often, and which has 'privacy settings' or different privacy options. Ideally, not all pupils should use the same, so there will be different services to compare. Nonetheless, some pupils could work in parallel or together on the same service.

- Second, **describe** how the service works if the user does not actively change anything: in other words, what are the '**default privacy settings'**? What would happen if you just register? Will your profile information be online and accessible to everybody through search engines? Does this profile information include data that such as your real name, date of birth, a picture of you with your face? What will automatically happen to the data or pictures you send to others or post using your account?

- Third, **detail** which privacy options are available to users: What can you actually change? Can you set your profile to private? Can you share info with only a few people? Do you really control who will access the data?

- If there are pupils who do not use any online service or application with privacy settings at all, they could, as an alternative, work on their **offline practices of sharing information**: What information about them is available to people as they walk on the street? What information or pictures do they share with others? Could they change their 'privacy settings' if they wished? How? They could

think for instance of: wearing sunglasses, sharing information with somebody only if they promise not to tell to anybody, etc.

- Finally, **share, compare** and **discuss** the results of the different explorations. Consider these questions: Were the pupils fully aware of the 'privacy settings' of the services they use? Do they think they really allow them to control their data? Are they easy to find, and easy to use?

2. ***How do we shape our privacy?*** This exercise should work as an invitation for younger children to think about the ways in which we manage daily of privacy preferences and requirements – and the different 'tools' and strategies we use:

- In small groups or on their own, pupils should **list** different groups of people depending on what kind of information they share with them: for instance, 1) mum & dad; 2) siblings; 3) friends; 4) other pupils; 5) teachers and other adults they know well; 6) unknown people on the street. (There might be also other categories, such as 'really best friends', 'neighbours', 'grand parents and other members of the family', 'favourite doll', etc.: children should figure out themselves which are the relevant groups for them);

- For each group, pupils should **enumerate** information that they would only share with that group. For instance: Are there things you would only tell your (best) friends? With whom would you OK to be in your pyjamas? Are there some kinds of information that you think your teacher should know, but probably not strangers on the street?

- The class should **put in common** their answers, and talk about **how do we actually make sure** that we share what we want with only the people we want. For instance: we do not go to the street in our pyjamas, we speak with some people about certain things only when nobody else is around, sometimes we speak softly, sometimes we ask people to promise to keep a secret, etc.

- The teacher should **explain** that privacy is about controlling who knows what about us, and that, just like we make an effort to control this in our everyday life, when people go online they should also remember to control what they share with whom.

For the youngest

Youngest children should learn that, just like there are some people who could be tempted to steal their stuff, there are some people who would like to steal their data. They shall thus be careful with what they do with it, think about where they store it, and never give data about them to strangers.

For the most advanced

The most advanced pupils should learn to act responsibly with their data: have strong passwords, keep them private, and beware of phishing. They should also know well the 'privacy settings' of the services or applications they use.

8. Family, privacy and personal data protection

Parents can be very useful to help children protect their privacy and personal data. Sometimes they could also, however, be a bit too invasive.

Objectives

This chapter aims to help pupils to:

- Learn about how their parents can help them in protecting their privacy and personal data.
- Think about whether parents can also infringe their privacy, and what to do about it.
- Suggest opening a discussion with their family.

By reflecting upon these issues, pupils will engage in thinking about the data they produce, and who can access it.

Key issues

Parents can play a **crucial role** in the protection of privacy and personal data of their children. While children are unable to consent to some personal data practices, it is generally the parents (or guardian) that will have the capacity to **refuse or consent** to those practices.

This does not mean, however, that parents should take these decisions without taking into account the children's wishes. On the contrary, parents should listen to their children, and help educating them so they can in the future **take the right decision** about what to do with their data. Parents should thus **help children defend their rights** and help them learn how to do so.

In practice, however, it can happen that parents are unfortunately actively playing an actively role in **infringing** children's privacy and personal data protection rights:

- Parents certainly need to know about some of their children's activities to ensure their safety and education – which is their responsibility. Their **surveillance**, however, can sometimes go too far and unnecessarily invade too many spaces of their children's lives. In some cases, children are unaware of how they are being tracked, which is particularly problematic.

- Parents can also '**over-share'** information about their children with other people. For instance, some parents post pictures or videos of their children to social media without controlling who has access to them, or without realising that these images could be indefinitely linked to their child's name. These pictures and videos might look sweet to them, but could, in other contexts and some time later, generate embarrassment, or even be misused.

When they feel uncomfortable about any of these issues, children shall be able to **talk about them** with their parents. They should be granted at least of some zones of **privacy** and be made of **aware** of how the data about them is used. As they grow, they

should be granted more power in deciding what happens to their data, and certainly have a say on the pictures, videos, or any information about them posted online.

Real life case

Some users of the photo-sharing social networking service **Instagram** launched the trend **#BabyRP**, a sort of role playing where people play the roles of 'baby', 'mum' and 'dad' by using pictures of real babies and children that they take from other users, without asking them permission. In some cases, the real parents discovered that strangers had been using their children's images only after these had been shared widely by their fake families, with fake names and in imaginary situations.

Ideas for discussion

Pupils can be asked to discuss these questions:

1. ***Personal experiences***: Have you ever felt that your parents invaded your privacy? When? What did you do about it? Sometimes, parents interfere with their children's privacy without even realising it: for instance, during a dinner with other family members or friends, they could share an anecdote about their child that they think is very sweet or just funny, but that their child finds extremely embarrassing. Do you think your parents have the same ideas as you on what needs to be kept private?

2. ***Looking for rules:*** Do you think parents have the right to monitor their children's activities? Why should they need to do that? Should there be any limits to their surveillance? Should rules be different depending on the age of the child?

Recommended activities

1. ***Acceptable practices?*** This exercise can help pupils think about what their parents know about them and about their behaviour. Pupils should:

- **List** the ways in which parents could, in general, track their children's activities. Think for instance about checking their online behaviour, keeping an eye on their phone communications, accessing their social media accounts, monitoring how they spend their (electronic) money, etc.

- **Underline** the practices that, in their view, are not acceptable.

- **Compare** the answers with the other pupils' answers. If there any differences, explore why.

2. ***You teach them.*** Sometimes it can be difficult for parents to support their children in protecting their privacy and personal data protection because they know little about the devices and services that their own children use daily. This exercise aims to encourage the class to think about this problem, and to realise that maybe they have some very valuable knowledge that they could use to digital empower the whole family. Pupils, on their own or in small groups, should:

- **Imagine a lesson** about a device, social networking platform, application or any other digital service that they enjoy very much using and know very well,

but that their parents do not use at all, or do not know that well. What should their parents know if they were to use it? Why is it so useful, or such fun to use it? Describe how it functions, and what are its advantages.

- **Include in the lesson some privacy tips** for the parents, so they can protect their privacy and personal data when using it: Should they create an account using their real name, or preferably not? Are there any privacy settings they can change? Will a company be collecting data about them? Who will see the info they share?

For the youngest

Youngest children should be clearly made aware that they their parents have a key role in helping them protect their privacy and personal data. If they ever feel their parents are invading their privacy, or not protecting their rights as they would like them to do it, they should talk without them about this. The parents could have a good reason for doing what they do, or, in some cases, not have realised that they were interfering with their children's privacy.

For the most advanced

The most advanced pupils should know that their parents have a key role in helping them protect their privacy and personal data, but that they also have a crucial role to play, and that their views on these subjects do matter.

9. Keeping safe, feeling good

Through the Internet we may come across things that hurt us, as well as people that are not particularly nice or considerate, or even individuals with bad intentions. Children should make their best to avoid predictable dangers, as well as avoiding any behaviour that could hurt others.

Objectives

This chapter aims to help pupils to:

- Consider possible risks online.
- Think about '**cyber bullying'** and online '**hate speech'**.
- Think about the possible dangers of **'sexting'.**
- Prevent risky behaviours.

Key issues

Online, just like in the offline world, **not everybody is your friend**. Through social networks, in online games, or just by commenting things online, you could come across people that look very friendly, but this does not mean you should trust them. Children and teenagers must be aware that, just like they would not go and tell their personal life to strangers on the street, they should never give any confidential information to strangers online. This notably includes not giving anybody **phone numbers** or **addresses** that people could later use to bother them.

As a matter of fact, just like in the offline world, online even your friends can sometimes hurt you. We know indeed that people can sometimes behave in strange ways when they communicate online, perhaps because they think nobody sees them, or because they are not completely aware of the **implications** of their online behaviour.

Sometimes, people hurt other people on purpose. We call **'cyber bullying'** the action of harming or harassing somebody through the Internet, in particular when done on purpose and repeatedly. There are actually many types of cyber bullying, ranging from spreading false rumours through social media to continually annoy somebody by pestering them.

All these behaviours can have **dramatic consequences** on the victim. It is thus crucial that minors do not engage in any activity (like posting, commenting or sharing) that could be experienced as 'cyber bullying' by anybody, and that they are ready to support their peers if any of this happens to them. If they go through the situation themselves, they should be able to talk to their parents (or guardian), or a responsible adult, to make the situation **stop** as soon as possible.

A particularly disgraceful way of hurting others online happens when people attack a person or the group they belong to because of their gender, their ethnic origin, their religion, disability, sexual orientation… or any other 'difference' that they wrongly perceive as giving them a reason to be degrading. This is sometimes called '**hate speech'** and is not only vexing for the person attacked, but also for the whole group of people concerned. Minors should be aware acting like this is wrong, and that the

law foresees sanctions for those who do it, so they should actually report 'hate speech' whenever they encounter it.

Finally, pupils should consider the possible dangers linked to **'sexting'**, or the practice of sending and receiving of sexually explicit photos, messages or videos – be it by text messages, emails or through social networking sites. Teenagers who might be tempted to send or receive this kind of images often do not have a clear perception of the many ways in which the photos, messages or videos might turn up in the wrong hands: they should thus be reminded of the fact that whoever gets access to such a piece of information might share it further or even make it publicly available to everybody, just **by being negligent**, **by mistake**, **as a (bad) joke** or **even on purpose to** unsettle them. In addition, teenagers often do not imagine the possible **major negative implications** of these scenarios, which could leave them vulnerable to much embarrassment, or even to blackmail.

Definitions

Cyber bullying

Ideas for discussion

1. ***Personal experiences about cyber bulling (and how to stop it).*** Pupils should address these questions: Have you ever come across anything that looked to you as 'cyber bullying'? What did you do? Some experts says that in those situations people should try to show the victim of cyber bullying that they support them, and that they are not intimidated by the bullies. Is that easy to do? What else can be done?

2. ***The most private things.*** Pupils should engage in a discussion about the dangers linked to **'sexting'** by considering, for instance, an imaginary scenario like this one:

- **Scenario**: An imaginary girl, called G, and an imaginary boy, called B, both teenagers, decide to celebrate their anniversary by exchanging sexually explicit images of themselves, because they have read it could be fun. They promise each other they will not share them with anybody. The day after, the boy goes to the swimming pool and accidentally forgets his phone in the changing room, outside the locker. While he is swimming, another boy sees the phone, check its content, finds the picture of the girl, and decides to share it through a very popular social network, using the account B's account – that is, to all his online 'friends'. He then leaves the phone where it was, and goes away. In the meantime, G, who was just about to write on her blog about her latest holidays, suddenly sees the picture pop up through the social network, apparently sent by her boyfriend's profile. Almost immediately, she starts receiving mocking and degrading comments from people, including people who were not B's online 'friends'. Very angry and extremely disillusioned, she decides to take revenge by posting on her blog, that is, open to everybody, B's picture, and sends an email to B's father (whose email address she finds online), to make sure he is aware of it.

- **Discuss:** What could happen next? Is there anything G and B could have done to avoid this situation? What exactly? Do you think this scenario could actually happen in real life? If not, what kind of problematic scenarios can you imagine?

Recommended activities

1. ***Think before you share***. There are many reasons why some unsuitable information might be posted online by children or teenagers without much prior thinking about the consequences. For instance, children may think it is just funny to share publicly a picture where their friends look ridicule or weird, without realising that the picture could be shared again and again and become widely exposed, which their friends will not find funny at all. Or, in a moment of anger, minors could feel like writing online something particularly nasty about somebody, without realising that this may not only upset the attacked person, but actually also poison their daily life for a long time. This exercise invites people to **reflect** upon those cases. Pupils should:

- **Describe** situations where they could imagine that somebody would share or post online information that would later become a problem, and what kind of problematic content could find its way online: for instance, teenagers at a party could share pictures of behaviours that should only be known to those who were there, friends who have an argument might tell secrets they were not supposed to tell,

- **Discuss** what could be done to prevent problems: Are there any types of data that one should never share? Would always asking for other people's permission before using data about them be a good idea?

For the youngest

Youngest children should know that through the Internet they could run into all sorts of people. Even when these strangers or new 'friends' look friendly, one cannot be completely sure they deserve trust. Children give should never to strangers or online 'friends' any personal data such as their telephone number or postal address, or any pictures.

For the most advanced

Most advanced pupils should adopt a reflective attitude towards their online behaviour. They should remember to always ask themselves if the information they share or post could have a negative impact on somebody (including themselves, but not only!), for instance if it was to be used in a different way than initially foreseen.

10. Taking action

Having the right to personal data protection means that you have some rights that you can use, so you should not be afraid to use them – directly or with the help of an adult. In case of doubt, contact your data protection authority for guidance. And, in case of urgent problem, you should know who to contact too.

Objectives

This chapter shall help pupils to:

- Master their **personal data protection rights**.
- Know **what to do** when an organisation does not respect their rights.
- Be aware of the existence of a **data protection authority.**
- Know **whom to contact** when they face a difficult, urgent situation.

Key issues

Anybody whose personal data is being used by an organisation or a company has the right to ask them **which data** they have, to make them **rectify** the data if inaccurate, and to have them **delete** the data if there is no need for them to have them. If you **consented** to a company to get your personal data but later change your mind, you can inform them and they should also take immediately the necessary steps to **delete** the data. These are everybody's basic **personal data protection rights**, which everybody should be able to use directly by addressing the company that has data about them.

If a company sends you commercial messages, or keeps calling you, and you are not interested in what they want to tell you, you can **tell them to stop**. Often this is done by 'unsubscribing' to their mailing list. All commercial messages should explain clearly who is the sender and how to tell them to stop sending information.

Particular young children are not supposed to exercise their personal data protections rights on their own, but they can **ask their parents or guardian, or a responsible adult**, to use them to effectively protect their data.

If the company or organisation that is using the data does not react appropriately, or does not respect people's choices, it is possible to contact a **data protection authority.**[1] This is an agency especially working to make sure that personal data is always processed following the existing rules, and that whoever use people's personal data respects people's rights.

The **data protection authority** can offer guidance and, if necessary, help to introduce a complaint. They might also get in touch with the company or organisation, and perhaps solve the problem.

[1] All national data protection authorities, listed by country, can be accessed through this link: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm

Some situations, however, need much **urgent action**, and cannot be tackled by data protection authorities. Minors sometimes discover that somebody has shared online information about them that can cause much distress, and that must be removed immediately. Sometimes this happens by mistake, and sometimes it happens because of ill-intentioned people, who will not cooperate in taking down the information.

In all these cases, children and teenagers can try to get the information removed as quickly as possible by contacting the website or the service provider, like a social networking platform. As this can sometimes be difficult, they should not be afraid to talk about it with **their parents or guardian, or a responsible adult**, who should be able to assist them.

If they prefer, minors can also directly contact an **Insafe helpline**. These are helplines specialised in giving a hand to children and teenagers when they go through difficult online experiences or encounter inappropriate content, and are generally accessible for free and anonymously.[2] They can also be of help in cases of **online harassment**. In case of serious problems, minors should not hesitate to contact **the police**.

Recommended activities

1. ***Using your rights for real:*** This exercise requires some time (a delay of at least some weeks needs to be foreseen to wait for replies), but it can be particularly useful for pupils to actually experience what it means to have a right to personal data protection. Each pupil shall:

- **Chose** a company or organisation that they think could have personal data about them.
- **Write down** why they have picked up that particular company or organisation, and which data they think they have about them.
- **Make use of their right of access** by contacting the company or organisation, and asking them to tell them which data about them they have.
- **Wait** for an answer for at least a few weeks.
- **Explain** to the class which entity they contacted, why, which data they thought they had, whether they received an answer, and what did they find surprising about it, if anything.
- **Compare** their own experiences with that of the other pupils. In light of all the results, consider these questions: Can it be useful to exercise the right of access to your personal data? Why? Is it easy to get a reply? Could the data protection authority be of any help?

For the youngest

Younger children should know that they can **exercise their control on data about them** with the **help** of their parents or a responsible adult, and that there exists a **data protection authority** that has the mission to ensure that everybody complies with

[2] All national helplines, listed by country, can be accessed through this link: http://www.saferinternet.org/helplines.

personal data protection rules. They should also know that if they ever find online something that disturbs them, it is better to call for help.

For the most advanced

Most advanced pupils should know which are their **personal data protection rights**, and feel comfortable with the idea of **exercising them**. They should understand that they have the right to speak up if they think that somebody is misusing data about them, and know there is a **data protection authority** that can give them more information or guidance. Additionally, they should know that if they are in trouble due to something that is online, adults can help them.

11. Glossary

Behavioural advertising: ads that are displayed because, on the basis of the data previously collected about the user, they seem to have many chances of having an impact on them.

Consent: the freely given, specific, informed and unambiguous expression of acceptance of some uses of personal data, given by the person associated with the data.

Cyber bullying: harming, tormenting, harassing or threatening somebody using technology, in particular when done on purpose and repeatedly.

Data controllers: the entities responsible for the processing of personal data.

Data subject: the person that can be associated with some personal data, and has a series of rights upon such data.

Digital identity: the image of people as it can be built with online information about them.

Identity theft: impersonating somebody, in particular by gaining enough information about a person to be able to pretend to be such individual.

Personal data: any data that can be connected to a person, as long as we know who is this person. The data can take any shape: it can be written information, an image, a sound, a fingerprint, etc.

Phishing: the attempt to obtain information such as usernames, passwords, or credit card details by masquerading as a trustworthy entity in an electronic communication, typically by email.

Profiling: process where information about a person is gathered and analysed. Based on this information individuals are put in categories/profiles that are composed of people with similar characteristics, preferences, activities. Additional information about people may be assumed or implied based on the collected data.

Right to privacy: traditionally described as 'the right to be let alone', this fundamental right is a actually a broad notion that protects the confidentiality of communications, the inviolability of the home, family life, personal data and, generally speaking, everybody's right to life their own life, free for undue interference.

Right to the protection of personal data: this fundamental right protects people by giving them a series of rights on the data about them processed by others, imposing on those a series of obligations, and establishing a data protection authority to monitor compliance with the rules.

Sensitive data: data deserving reinforced protection, such as data about peoples' beliefs, their health, their ethnic origin or their sex life.

12. Useful resources

- National data protection authorities, by country: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm

- National Internet helplines, by country: http://www.saferinternet.org/helplines.

The first ARCADES deliverable, publicly available online, provides detailed and useful links information about relevant teaching initiatives and resources. See: Gloria González Fuster, Paul De Hert, and Dariusz Kloza (2015), *Deliverable 1.1: State-of-the-Art Report on Teaching Privacy and Personal Data Protection at Schools in the European Union*, ARCADES.