Office of the Information and
Privacy Commissioner of Alberta

COURIER

November 8, 2017

Honourable David Eggen
Minister of Education
228 Legislature Building
10800 – 97 Avenue
Edmonton, AB   T5K 2B6

Dear Minister Eggen,

Re: Privacy Education

In an open letter to the Council of Ministers of Education on November 3, 2017, my colleagues across Canada and I called on provincial and territorial governments to include privacy education as a component in digital literacy curricula.

The open letter (attached) draws attention to the International Competency Framework on Privacy Education, which was adopted by participants at the 38th International Conference of Data Protection and Privacy Commissioners in October 2016.

In light of the open letter, I would like to share with you some work being done in Alberta to enhance privacy education. Educating youth on access and privacy issues is part of my office's strategic business plan, and several initiatives are ongoing, including:

- **The eQuality Project:** My office supports The eQuality Project, which is a seven-year research program that aims to promote healthy relationships and respect for equality online. In addition to the project's digital privacy component, a goal is to reinvigorate the cyberbullying debate. The Alberta Teachers' Association (ATA) and Alberta Status of Women are official partners in the project, as well as policymakers, community organizations, scholars, educators and youth from across Canada.

  My office co-hosted an event on "Privacy Implications of the Networked Classroom" with The eQuality Project and the ATA in January 2017 for Data Privacy Day that included participation by researchers, Alberta teachers and school administrators, and access and privacy professionals. It helped to provide project leaders with a base of "on the ground" research from Alberta. A follow-up public lecture was hosted by the ATA's Educational Technology Council.

The eQuality Project is currently in year two, and it aims to not only develop new knowledge and research to inform policy decisions at the provincial and school board levels, but to also publish education materials to help young Canadians make the most of their digital media experiences.[1]

- **Alberta Education Curriculum Review:** In May 2017, I had the honour of presenting to the Alberta Education Curriculum Review Working Groups to state the importance of teaching students about privacy rights in the digital economy and to share with them some of the resources available across the country and internationally with respect to privacy education, including the International Competency Framework on Privacy Education and a Kids' Privacy Sweep Lesson Plan my office developed in partnership with the Office of the Privacy Commissioner of Canada.

- **School at the Legislature:** My office continues to participate in the School at the Legislature program hosted by the Legislative Assembly Office. We recently redeveloped the presentation to focus primarily on digital privacy rights and the importance of privacy education in the information economy.

- **Presentations to Education Stakeholders:** Over the past year, I have been invited to speak to other stakeholders in Alberta's education sector, including the Alberta School Boards Association and the Association of Independent Schools and Colleges of Alberta. My office continues to receive interest from school district administrators and schools to present to staff and/or students about information and privacy rights in the information economy.

There seems to be a general consensus in response to these initiatives: Students require skills and knowledge to safely navigate their networked world, and to understand how to uphold information and privacy rights in the digital economy.

This is why I believe the comprehensive curriculum review process you have undertaken is timely for the work my colleagues and I across Canada are engaged in. I would like to reiterate the invitation in the open letter to CMEC by welcoming the opportunity to meet with you and other appropriate officials in your department about this important topic.

To complement the open letter, I intend to post this letter on my office's website at www.oipc.ab.ca.

Sincerely,

Jill Clayton

Jill Clayton
Information and Privacy Commissioner

CC: Honourable Stephanie McLean, Minister of Status of Women

[1] More information about The eQuality Project is available at www.equalityproject.ca/about/our-project/.

Office of the Privacy Commissioner of Canada

Information and Privacy Commissioner of Ontario

Commission d'accès à l'information du Québec

Office of the Information and Privacy Commissioner for Nova Scotia

Office of the Integrity Commissioner for New Brunswick

Manitoba Ombudsman

Office of the Information and Privacy Commissioner for British Columbia.

Office of the Information and Privacy Commissioner of Prince Edward Island

Office of the Saskatchewan Information and Privacy Commissioner

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and Privacy Commissioner of Newfoundland and Labrador

Office of the Information and Privacy Commissioner of the Northwest Territories

Yukon Information and Privacy Commissioner

Office of the Information and Privacy Commissioner of Nunavut

November 3, 2017

Council of Ministers of Education, Canada
c/o Honourable Melanie Mark, Chair
95 St. Clair Ave. West, Suite 1106
Toronto, Ontario M4V 1N6

Sent by email

Subject: Privacy education

Dear Madam Chair and members of the Council of Ministers of Education,

As federal, provincial and territorial privacy protection authorities, we are writing to you about an issue critical to young Canadians growing up in an era of unprecedented technological change with profound impacts on privacy.

As such, we are writing to encourage you to make privacy education a greater priority by including it as a clear and concrete component in digital literacy curricula across the country.

It is important that students become savvy digital citizens who are able to enjoy the benefits of being online. Young people need to be equipped with the knowledge necessary to navigate the online world and participate in the digital domain while protecting their privacy.

The risks associated with connecting to the Internet have grown exponentially in recent years. From cyberbullying, sexting and child luring, to tracking, hacking and email scams, the threats can be daunting for many adults, let alone children and teens. At the same time, personal information has become a hot commodity as businesses seek to monetize our data. It has become difficult to discern who is processing our information and for what purposes and everyone, regardless of age, must weigh the benefits and risks of each product and service they use, each time they use it.

A recent survey for the Office of the Privacy Commissioner of Canada found 92 per cent of Canadians are concerned about the protection of their privacy and nearly half feel as though they've lost control over how organizations collect and use their personal information.

These findings are alarming and can only be addressed if we help younger generations to develop skills that will allow them to navigate the ever complex digital environment safely and responsibly.

.../2

Although many schools across Canada currently teach digital literacy skills, they generally focus on personal safety risks or on acquiring digital skills for the labour market. With the exception of certain one-time initiatives, privacy is not necessarily a part of the courses offered, and many students graduate high school never having learned how to think critically about the information they emit into cyberspace or how to safeguard their digital footprint. This leaves them at unnecessary risk.

As data privacy regulators, we want to draw your attention to this critical issue, which is raising concerns worldwide.

Last fall, participants at the 38th International Conference of Data Protection and Privacy Commissioners adopted the Resolution for the Adoption of an International Competency Framework on Privacy Education. This resolution encourages governments, and especially authorities who are responsible for education and other stakeholders interested in the education sector, to champion the inclusion of privacy education in schools and to advocate for and develop training opportunities for educators in this area. Canadian privacy oversight offices attending the conference signed on to the resolution.

The framework adopted at the conference serves as a roadmap for teachers around the world, outlining nine foundational privacy principles students ought to know and understand. This includes being able to identify what constitutes personal information, being able to understand both the technical and economic aspects of the digital environment, knowing how to limit disclosure of personal information and how to protect oneself online. It states that students should also learn how to exercise their privacy rights and responsibilities as digital citizens.

In order to train young people and give them the tools they need to fully and confidently participate in the digital economy, and in addition to organizing one-time activities (e.g. posters, school tours), Canadian schools must take privacy into account in a more systematic way so that students are sensitized throughout their schooling. We believe part of the solution lies in ensuring digital literacy skills are taught in all schools across Canada, and that privacy education figures clearly within that curricula. Those who learn to protect their privacy, exercise control over their personal information and respect the privacy of others at an early age, will gain tools that will serve them well into adulthood.

In view of the above, federal, provincial and territorial privacy protection authorities strongly urge all those working in the education sector to take steps that will allow future generations of Canadians to develop these digital skills and to succeed in an increasingly data-driven world. To that end, we would welcome the opportunity to meet with appropriate officials from your departments in your respective jurisdictions. Additionally, a delegation representing the signatories below would request to meet with you jointly at an upcoming Council of Ministers of Education meeting.

As privacy advocates keenly interested in ensuring young Canadians grow up with privacy skills and knowledge, we would welcome the opportunity to provide any support you may find helpful.

.../3

This is an extremely important issue to our offices and we plan to post this letter on our websites next week as part of our efforts to draw public attention to the importance of privacy education in Canadian schools.

Sincerely,

Daniel Therrien
Privacy Commissioner of Canada

Brian Beamish
Information and Privacy Commissioner of Ontario

M^{e} Jean Chartier
President, Commission d'accès à l'information du Québec

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

Alexandre Deschênes, Q.C.,
Integrity Commissioner for New Brunswick

Charlene Paquin
Manitoba Ombudsman

Drew McArthur

Drew McArthur
Acting Information and Privacy Commissioner for British Columbia

Karen A Rose

Karen A. Rose
Information and Privacy Commissioner of Prince Edward Island

Ronald J. Kruzeniski, QC
Saskatchewan Information and Privacy Commissioner

Jill Clayton

Jill Clayton
Information and Privacy Commissioner of Alberta

Donovan Molloy, QC,
Information and Privacy Commissioner of Newfoundland and Labrador

Elaine Keenan-Bengts
Information and Privacy Commissioner of the Northwest Territories and of Nunavut

Diane McLeod-McKay
Yukon Information and Privacy Commissioner

Enclosures:

Resolution for the Adoption of an International Competency Framework on Privacy Education

Personal Data Protection Competency Framework for School Students

38th INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Marrakesh, 18 October 2016

Resolution for the Adoption of an International Competency Framework on Privacy Education

The 38th International Conference of Data Protection and Privacy Commissioners:

Recalling the international agreements specifically referring to children's rights:

- The Geneva Declaration of the Rights of the Child, September 26, 1924;
- The United Nations Convention on the Rights of the Child, November 20, 1989;

Having regard to the international recommendations pertaining to the education of children and adolescents, namely:

- The Recommendation Rec(2006)12 of the Committee of Ministers of the Council of Europe to member states on empowering children in the new information and communications environment, 27 September 2016;

- The Declaration of the Committee of Ministers of the Council of Europe on protecting the dignity, security and privacy of children on the Internet, 20 February 2008;

- The OECD's Recommendation of the Council on the Protection of Children Online, 16 February, 2012;

- UNESCO's Resolution on Internet-related issues, including access to information and knowledge, freedom of expression, privacy and ethical dimensions of the information society, adopted in November 2013 at the 37th session;

Referring to International Declarations, designed to encourage States, in their mid- and long-term efforts to foster quality education and to make education for all a priority, including digital education:

- UNESCO's 2015 Incheon Declaration, which defines the *Education 2030: Towards inclusive and equitable quality education and lifelong learning for all* Framework for Action, to promote in particular, global citizenship education by drawing on Information and Communication Technology (ICT);

Recalling the two Resolutions of the 30th International Conference of Data Protection and Privacy Commissioners in 2008:

- The Resolution on Privacy Protection in Social Network Services;

- The Resolution on Children's Online Privacy, which encouraged Commissioners to develop digital education programs in particular for young people;

Recalling the Resolution of the 35th International Conference of Data Protection and Privacy Commissioners in 2013, on Digital Education for All, which recommended that Commissioners:

- Promote data protection and privacy education in digital literacy programs;

- Participate in the training of relay persons, by organizing or collaborating on the "training of trainers" on data protection and privacy;

Realising that, for many States, digital education for school-aged children is today, at a national or sub-national level of governance, a priority for action;

Recognising that according to member jurisdictions, education policy aimed at schools rests with different levels of government and that privacy laws vary from country to country, and that this resolution can still be meaningful under these circumstances;

Considering that in order to effectively equip individuals to be active in today's digital society and digital economy, it is now important to raise children's awareness, as soon as they start school, of the implications of using and sharing data as well as on a common base of concrete and operational competences with regards to data protection and privacy; and that, in this regard, highlighting data protection issues as part of digital literacy education, tailored to domestic conditions, is an essential element of teaching citizenship and respect for human rights;

Recognising that, in spite of the quality of pedagogical resources produced with regard to data protection, there is a lack of training for educators regarding data protection and privacy, except in a few countries;

Recalling that the training of educators has an impact on the teaching of students and that schools must have the means to educate citizens on how to use new technologies responsibly and ethically;

Considering that, in collaboration with education professionals, government representatives, and other concerned stakeholders, data protection authorities, owing to their expertise, can make a useful contribution to this training;

Determining, in this regard, that it is necessary to propose a common base of concrete and operational competencies within an international Competency Framework for teaching school students on data protection and privacy, for educators

The Authorities present at the 38th International Conference of Data Protection and Privacy Commissioners consider it an important priority to recommend the following actions:

- Include data protection and privacy education in study programs and curricula ;

- Train educators on data protection and privacy by providing them both essential knowledge as well as practical expertise in this sphere, enabling them this way to help young people develop their critical thinking on how personal information is used;

- With this in mind, initiate training activities that are focused both on the benefits and risks involved in using new technologies and the practices that enable us to live in a digital environment with confidence, clarity and respect of individual rights.

Consequently, the present authorities:

1. Adopt the international Competency Framework for school students on data protection and privacy attached in annex and draw the attention of governments and, in particular, responsible authorities for education as well as other stakeholders working in the education field, to the importance of:

   - Promoting in cooperation with data protection authorities the use and the practical development of the Competency Framework, as part of study programs or curricula and training of educators, regardless of the discipline taught;

   - Encouraging research in pedagogy and didactics related to data protection and privacy, so that the development of activities and resources in this field is based on scientific studies and professional experience.

2. Mandate the International Working Group on Digital Education to:

   - Ensure that data protection authorities can propose or contribute to, in co-operation with their domestic government authorities and relevant stakeholders, the production of pedagogical resources tailored to the specific framework competence addressed and the age group concerned;

   - Ensure follow-up of progress made in the development of data protection and privacy competencies regarding digital education in educational programs.

The U.S. Federal Trade Commission abstains because the resolution adopts a single international framework without recognizing that other approaches reflecting the diversity of privacy laws and cultural values that exist around the world could also achieve the common aim of promoting digital education.

International Conference of Privacy and Data Protection Commissioners

Personal Data Protection Competency Framework for School Students

Intended to help Educators

October 2016

October 2016

Personal Data Protection Competency Framework for School Students

Intended to help Educators

Introduction and Acknowledgements

Why an international framework on data protection training?

In the digital age, responsible, ethical and civic-minded education in the use of new technologies is a priority for action, particularly for young people in school.

A key component of digital education is highlighting privacy and personal data protection. Educators have a key role to play in this digital education of citizens.

Acquiring critical knowledge and understanding of digital rights and responsibilities, developing critical thinking skills in young people towards the uses of personal data, raising awareness of risks, and teaching practices to enable people to navigate the digital environment with confidence, lucidity and respect for the rights of everyone – these are the learning objectives to be attained.

To assist educators, data protection authorities—with their expertise in this field—thought it necessary to design a training framework for students specifically dedicated to data protection, for use in official school programs and in training courses for educators, regardless of the particular discipline taught.

Although it can certainly be adapted to address specific educational purposes, laws and data protection approaches relevant to each country, the framework has been deliberately designed to have an international dimension.

Why? Because this is a major issue that concerns all countries without distinction; because it aims to create **a common base of concrete and operational competences about personal data protection** that can be used by everyone; and because its purpose is to address the world of education as a whole.

That is why this framework, designed on the initiative of the International Digital Education Working Group coordinated by the National Commission on Information Technology and Liberties (CNIL), was adopted by all the data protection authorities at the 38th International Data Protection and Privacy Commissioners' conference in October 2016[1].

About the Framework

The purpose of this set of learning principles is to provide all students the knowledge, competencies and skills identified in the common base of concrete and operational competences of the competency framework on data protection.

This framework presented here has nine ***foundational principles***; knowledge and understanding of these is a priority.

[1] Resolution of 18 October 2016 for the adoption of an international Competency Framework on Privacy Education.

A block of stand-alone general competencies is identified for each principle. They are juxtaposed and linked so that they achieve a progressive thematic balance. Nevertheless, educators will be able to use them, either by following the progression suggested in the document or in a modular manner, as part of their instruction.

Each of the principles was analyzed in terms of **knowledge and skills**, with the acquisition of the knowledge or skill affecting the student's ability to say "*I know*" and/or "*I can*." These **descriptors**, as well as what the terms "knowledge" and "skill" cover, are defined in the proposed terminology appended to this document.

The agreement reached on ***a common base of concrete knowledge and skills*** is the first step in disseminating and promoting the protection of personal data and privacy in education programs.

Other steps and action items are important to successfully achieve digital education efforts, which are:

- How educators implement these teaching principles in the classroom setting;
- The identification, **based on the age group considered**, of the degree of depth needed for each knowledge and skill element; and
- The availability of **training and education resources** to professionals and their students.

Further information at digitaleducation@icdppc.org

Acknowledgements to the contributors:

This framework has been designed by the French data protection authority, the National Commission of Information Technology and Liberties (CNIL), with the invaluable assistance of the data protection authorities belonging to the International Digital Education Group. It has also benefitted from the knowledgeable advice of education specialists and experts with the Educational Services of the Council of Europe.

Summary

[1/9] Personal data

Purpose: Understanding the concept of **personal data** is essential. The notions of **pseudonymity and masking one's identity** and **metadata** are also explained. The student is also taught that **certain personal data can be considered particularly sensitive,** because of the intimate nature of private life and/or the data could be the source of possible discrimination or they refer to minors. Finally, understanding the terms of data collection and processing is necessary to understand the concept of personal data.

KNOWLEDGE outcomes

- I understand what is involved in the concept of **personal data,** defined as any data—whether or not it was made public—about an identifiable individual;
- I know and understand the concept of **pseudonymity and masking one's identity;**
- I know that, **depending on how it is processed,** data may allow the identification of individuals;
- I know some **technical data** can assist in the identification of individuals; that scanned documents and images have embedded **metadata** that describe their contents and that online activity may leave **traces** (cookies, browsing history, etc.) which can contain personal data;
- I know that there are data **which can be considered as particularly sensitive, according to countries,** and which, for example, contain information regarding **minors, people's origins, political and/or religious opinions or affiliations, biometric or genetic profile, health and/or sex lives.**

SKILLS outcomes

- I can give examples of personal data that can directly identify individuals (civil status, photo of a student in the class, etc.) and technical data that can monitor the activities of a person and identify them (cookies, geolocation data, etc.);
- I can give examples of sensitive personal data (e.g., health, genetic profile, sex lives...).

[2/9] Privacy, civil liberties and protection of personal data

Purpose: The right to the protection of personal data is founded in **human rights, civil liberties, democratic values and citizenship**. It is also an important guarantee of **respect for privacy.**

KNOWLEDGE outcomes

- I know what human rights and civil liberties are and can recite them;
- I know these principles and democratic values are exercised as much in the real world as in the virtual world;
- I understand the concept of privacy, the right to privacy, and the need to have them recognized and protected;
- I understand how my actions may affect the privacy of others;
- I understand how the protection of privacy is not just about everyone's private life, but can also be applied in the public space, particularly on the Internet;

SKILLS outcomes

- I can give examples of situations pertaining to private life (e.g., medical consultations, parental separation);
- I evaluate what information I can and cannot disclose about myself and others (e.g., my home address, illness of a relative, etc.);
- I can give examples of situations in which digital media use has enhanced the expression of civil liberties and/or, *on the contrary*, curtailed them.

[3/9] Understanding the digital environment – technical aspects

Purpose: To protect his/her privacy, the student must understand the digital environment and must be able to navigate it independently. To do so, it is necessary to understand the **hardware** and **technical infrastructure of information systems** that support deployment.

KNOWLEDGE outcomes

- I know the difference between hardware, software and applications; I understand how **software and hardware components** make up computer systems;
- I know what the **Internet and its services** are (social networks, mobile applications, the cloud, etc.);
- I understand how digital space is structured (physical networks, browser, IP addresses and URLs, search engines, etc.);
- I am aware of the concept of information **architecture**, and the **collection**, **structure** and **processing** of information;
- I know the key **IT risks;** I know what **digital security** includes and understand the need to ensure the physical and logical security of a digital environment.

SKILLS outcomes

- I assess my practices and develop **problem-solving** and **learning** reflexes— namely about security—by identifying resources (user communities and forums, tutorials, etc.);
- I can identify malfunctions and solve simple problems by following established procedures; if necessary, I know how to actively seek solutions online, particularly when it comes to ensuring the security of my digital environment.

[4/9] Understanding the digital environment - economic aspects

Purpose: Understanding the digital environment and navigating it independently require **understanding it as an *ecosystem*** and **understanding its underlying logic**; this involves knowledge and competencies: the economics and ***value*** of personal data, key players and services, and economic models.

KNOWLEDGE outcomes

- I know who the key players in the digital economy are (e.g., ISPs, service providers, developers, curators, etc.);
- I understand the systems used to market products and offer **free services** (loyalty cards, targeted advertising *via* cookies, setting up user accounts, subscribing to newsletters, etc.), for the purpose of establishing **personalized user profiles**;
- I understand that the majority of such offers of services entail collecting and using personal data as well as storing this information in a database;
- I know what **data** are collected and stored when I use the Internet, a social network or a service.

SKILLS outcomes

- I can give examples of the types of technical data likely to be collected when I am online (e.g., browser type, contacts list, geolocation data, private messages, etc.).
- On any given website, I can find the **terms and conditions of use** of my personal data (Terms and Conditions of Use, legal information, privacy policy, etc.).
- I can give examples of digital services whose economic model involves—or does not involve—the collection of personal data.

[5/9] Understanding personal data regulations and legislation

Purpose: Knowledge of **data protection systems and institutions** is covered in this competency principle: *regulation principles*, applicable legal texts, Data Protection Authorities (DPAs). The student understands that in a ***number of countries*, personal data is protected by laws and regulations**, which means that individuals or **organisations** are not free to use it as they please.

KNOWLEDGE outcomes

- I know that personal data cannot be used for just any purpose and that regulations exist;
- I know and understand **the key rules relative to data protection:**
  - Personal data is processed or used for specific purposes and must be relevant to or consistent with the activity in question (e.g. finality, proportionality);
  - Some particularly sensitive data can be, in certain countries, be regulated in a specific way (e.g. data from minors, people's origin);
  - Personal data should not be retained for longer than is necessary and must then be archived or deleted (retention period) when appropriate according to countries's Privacy laws ;
  - People have rights regarding their personal data (e.g. access, correction, , refusal, consent);
  - Personal data is collected and processed or used under conditions that ensure privacy;
- I know that public and private organizations that collect and process or use personal data must comply with these rules and that violations can lead to **sanctions, according to countries;**
- I know of the existence, role and powers of **Data Protection Authorities;**
- I know that people about whom personal data is collected must **be informed** on their rights and of the use to which their data will be put and to whom it may be shared.

SKILLS outcomes

- I can give examples of digital practices that I think **comply** with and/or **violate** data protection regulations;
- I can name the Data Protection Authority in my country (of my area) or give an example of a Data Protection Authority, and I can cite examples of actions or decisions made by the authority;
- If a Data Protection Authority exists in my country, I can contact it for information and advice.

[6/9] Understanding personal data regulations: Controlling the use of personal information

Purpose: The student is taught that **the controlled use of his/her personal data** is both necessary and legitimate, based on the context in which it is used in daily life (as a student, team member, member of a family, etc.). The way that the student identifies him/herself and/or makes him/herself known to others in the digital world can vary depending on the situation and lead them to reveal more or less information about themselves. This is learning to manage one's "digital identities." Students are also introduced to the fact that they have rights and duties, particularly towards others.

KNOWLEDGE outcomes

- I understand the need and purpose of providing or not providing personal information, depending on the context and the end use of the information;
- To this end, I know how to set up and use pseudonyms and more than one email address, account and/or profile **depending on how I intend to use them.**
- I know that it is necessary to regularly monitor what is said about me online (my e-reputation);
- I know that posting involves **responsibility on my part** and that of my parents / legal guardians.

SKILLS outcomes

- I am careful to only share the personal data that is absolutely necessary to register for a service;
- I can express myself online while taking into account the **nature of the space** in which I am posting (private, public, related to school, family, friends, etc.);
- I am **vigilant about what I publish online**, even under a **pseudonym**;
- I can participate in an online debate with **respect for others**: I do not share information and photos of third parties without their knowledge and that can harm their privacy or reputation;
- I use tools to regularly monitor content and information about me that is seen by others on social networks.

[7/9] Managing my data: Learning to exercise my rights

Purpose: Here we learn about the range of actions available to me as a child/teenager *when it comes to consenting to or refusing the collection of my personal data,* **alerting, reporting** and protecting myself—through **intervention by a responsible adult**, when appropriate (*)—to deal with situations experienced and/or identified as breaching the privacy and/or the integrity of persons, or which constitute a violation of the law.

(*) By introducing the concept of **intervention** by a responsible adult and/or legal guardian, the authors take into consideration the specifics of national legislation, services offered, age group, child's level of autonomy and identified practices.

KNOWLEDGE outcomes

- I know that, to use certain online services, the consent of myself or my parents/legal guardians **is required**;
- I know that I have **rights regarding my personal data (e.g. access, correction, refusal, consent, delisting, erasure)** and that I can exercise these rights or have them exercised on my behalf by contacting the service in question according to domestic procedures and, in the event of a refusal or any problems, by contacting the Data Protection Authority if it exists, a judge, according to countries and/or the relevant national/sub-national authorities, or advocacy groups.

SKILLS outcomes

- I can update or request updates to data concerning me which appears to be **outdated, inaccurate or incomplete**, if necessary.
- I can request the deletion of my personal data online;
- I am able to check with the service in question whether or not personal data have been **collected and stored in a database**. If necessary, I can obtain this information from the service in question and exercise - or have exercised on my behalf - my other rights regarding said service;
- I am able to unsubscribe from a service and/or delete an account that I have created.

[8/9] Managing my data: Learning to protect myself online

Purpose: This competency principle covers the solutions used to **ensure the technical protection** and **security of personal data**. These solutions are the subject of **learning processes** experienced within the collective framework of school and school-related environments. Students must know how to use technical devices to identify and authenticate themselves online, authorize - or not - the collection of personal data, and set up an account and/or profile in accordance with data protection rules.

KNOWLEDGE outcomes

- I know that there are **ways to protect myself online**: in particular, I am familiar with the different ways to **identify and authenticate** myself; I am aware of data encryption solutions;
- I understand **the terms and conditions** of use relative to online services (allow or refuse geolocation, allow or refuse applications access to my contacts, photos, etc.);
- I know that I can **manage the settings** of the online applications and services that I use.

SKILLS outcomes

- I use procedures available **to protect my personal data**: for my accounts and profiles I can create strong passwords, or passphrases, and change them regularly; I can examine documents and images that I share online and if necessary, I can use tools to delete metadata; and data encryption solutions;
- I can manage the **security and privacy settings** of the accounts, profiles and devices that I use; I **regularly check** these settings and **adjust them**.

[9/9] The digital world: Becoming a digital citizen

Purpose: Students are to develop a critical and ethical approach to navigate the digital environment with **confidence and clarity** and act accordingly. Exercising their rights, using digital services while respecting the protection of personal data, identifying service offerings that may affect privacy or freedoms, reporting, and mobilizing: all actions which define a digital citizen, responsible for their own data and respectful of the data of others.

KNOWLEDGE outcomes

- I can compare information and **assess whether or not it is reliable**;
- I can **analyze and critically assess** a situation related to the use of digital media (e.g., the spread of false information and/or rumours);
- I can identify inappropriate or illegal content and behaviour;
- I can recognize situations involving **reputational damage** or **cyber-bullying**.

SKILLS outcomes

- In the situations described above, I can, directly or through an adult, **notify the relevant authorities and/or advocacy associations**;
- I am able to foster positive outcomes (complaints likely to influence major Internet players, mediation to ensure that inappropriate behaviour stops, development of codes of conduct, etc.);
- I am able to judge whether it is **appropriate** to publish such information **in a given context**; I can analyze and foresee the potential consequences of sharing it online.

Glossary (coming)