OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

Privacy Toolkit
OCDSB Privacy Week

November 12–17, 2018

OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

Privacy begins with you.

Understand Personal Information And Privacy

Privacy is the **right to control** access to your personal information and the **right to decide** what and how much information you give to others, who it is shared with and for what purposes it is used.

Personal information is recorded information about an individual that makes the individual identifiable, including: name, address, phone number; race, ethnic origin, or religious or political beliefs or associations; age, sex, sexual orientation, marital status, or family status; any identifying number (e.g. Social Insurance Number, OEN, student number); fingerprints, blood type, or inheritable characteristics; medical history; educational, financial, criminal, or employment history; personal views or opinions, except if they are about someone else; or anyone else's opinion about that individual.

Privacy and Personal Information are protected by law in Canada and Ontario through the **Education Act, Personal Information Protection and Electronic Documents Act (PIPEDA)**, and the **Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)**.

All employees of the District have an obligation to protect personal information about students and staff and should familiarize themselves with District policy P.128.GOV Privacy – Municipal Information of Information and Protection of Privacy Act and procedure PR.669.GOV Privacy Breach.

PROTECT PERSONAL INFORMATION

Follow these tips to keep personal information secure in compliance with the municipal freedom of information and protection of privacy act:

- Don't share your password with anyone;
- Only collect necessary personal information;
- Only access the personal information required to fulfill a business need;
- Consider privacy and the protection of personal information when planning projects, events, or field trips;
- Lock your computer screen when you are away from your desk to prevent the exposure of personal information;
- Don't leave documents containing personal information exposed on your desk or other public areas;
- Immediately retrieve documents containing personal information from the printer;
- Always double-check the names and addresses of recipients before distributing personal student or employee information by envelope or by email;
- Only discuss IEPs, IPRCs and Assessments with those who are involved in the process;
- Before installing or signing up for apps, understand what personal information is collected/shared and confirm classroom use with your principal;
- Use the bcc function when emailing multiple people; and
- Keep your devices secure and report lost or stolen devices to Business and Learning Technologies immediately.

REPORT A SUSPECTED PRIVACY BREACH

A **privacy breach** occurs when personal information is collected, used, disclosed, retained or destroyed in a manner that does not meet privacy requirements set out in federal and provincial legislation. Examples may include, but are not limited to:

- Memory key/jump drive containing student information is left in a public area;
- A laptop containing student records on the hard drive is lost or stolen;
- Documents containing student or employee personal information are left unattended on a photocopier or printer;
- Reports containing employee personal information are found un-shredded in recycle bins;
- Confidential documents are left in public view or on an employee's desk, computer screen or in a publically accessible area; and
- An unauthorized individual gains access to an information system containing student or employee personal information.

If you suspect a **privacy breach** has occurred you must:

- **Contain**, if possible, the suspected breach by delaying or stopping the process , activity or circumstances involving the exposure or mishandling of student or employee personal information;
- **Immediately notify** your supervisor and the District Freedom of Information Coordinator, Michele Giroux, Executive Officer, OCDSB;
- **Document** all steps taken and complete the *OCDSB Privacy Breach Report form;* and
- Following your report of the suspected breach, the FOI Coordinator may contact you to confirm details about the suspected breach.

Questions? Contact Michele Giroux, Executive Officer, Ottawa-Carleton District School Board
email: *michele.giroux@ocdsb.ca* office: 613-596-8211 ext.8607

OTTAWA-CARLETON
DISTRICT SCHOOL BOARD

Protect Your Privacy.

Your privacy is valuable and needs protecting.
Learn more about privacy rules at OCDSB policy P.128.GOV

Inform yourself on how to Protect your privacy.

Personal information is anything that could ID you, including your name and DOB, address, email, phone number.

Know the consequences of what you do and say online.

Your digital identity is forever.

Think before you open email or attachments.

IF IT LOOKS SUSPICIOUS, REPORT IT AND DELETE IT.

DO NOT OPEN IT!

Know what info is being collected about you.

Read the privacy policy for the app! Learn if they share your information with other companies.

Set the privacy controls.

Don't rely on the default — customize your settings.

Clear your browser history regularly.

Your history can be used to track and target advertising at you.

Use strong passwords.

No birthdays, pets or family names, and don't share or repeat passwords.

Think about what and who you share info with

There is no privacy on social media.

Protect information on all devices.

Use password protection on your phone, tablet and screen saver.

Secure documents.

Questions? Contact Michele Giroux, Executive Officer, Ottawa-Carleton District School Board
email: *michele.giroux@ocdsb.ca* office: 613-596-8211 ext.8607

Privacy Learning Activity

Each group will review an assigned text from pages 1 and 2 of this booklet. Working in your group, read the assigned text and answer the following questions. Please appoint someone from your group to act as recorder and make your notes on the blue sheet (these will be collected):

1. What were the 3–5 key things you learned from the text?

   »

   »

   »

   »

   »

2. Please list 3 questions or ideas that you have about how to be a better privacy steward.

   »

   »

   »

3. List some ideas that we can all use to promote this information during OCDSB Privacy Week.

   »

   »

   »

   »

   »

4. What other information, resources or supports related to privacy would be helpful to you?

Information, Resources, Supports	Identify any employee group with particular needs

Privacy Quiz

Q1	**Accidental Mix Up** An employee inadvertently mixes up the report cards for two students. A parent calls to say they received the information for another student.	**Is this a privacy breach?** ❒ Yes ❒ No
Q2	**The Stolen Laptop** You arrive at work and one of your staff advises that a laptop computer has been stolen from a car in the parking garage. The laptop was not password protected and contained the personal information of several hundred students.	**What would you do? Select all that apply:** A. Immediately contact your superiors and advise them of the event B. Contact the police C. Determine the scope of the breach D. Develop a privacy breach plan E. Notify the affected individuals F. Notify the Privacy Coordinator G. Contact B&LT and have the device locked down
Q3	**Privacy and Security** Which of the following statements about privacy is not true?	**Select the best response:** A. Privacy requires security B. Security requires privacy C. One can have excellent security but no privacy D. Informational privacy includes an individual's right to control the collection, use and disclosure of their personal information
Q4	**Personal Information** Which of the following are examples of personal information?	**Select all that apply:** A. An individual's name and address B. The student number assigned to an individual C. The name and business contact information of an employee D. Anonymous information that permits the drawing of accurate inferences about an individual E. An individual's name
Q5	**Sharing Student Information** You are developing strategies to support a student's learning needs. You want to consult with a colleague. What information is appropriate to share?	**Select all that apply:** A. Student name B. Educational history C. Date of birth D. Parent's marital status E. Nature of learning issues F. Details about previous suspensions

Q6	**Creating Forms** A notice of collection statement is required whenever personal information is collected. Which of the following must be included in comprehensive Notice of Collection?	**Select all that apply:** A. It must contain the name and contact details of a person who can answer questions about the collection practices of an institution B. It must include the legislative authority for collection C. It must indicate why the institution is collecting the client's personal information D. It must explain how the client's information will be used
Q7	**Sharing Personal Information** You are in the hallway and hear staff talking about an incident with a student. The discussion is explicit about the student's background and circumstances. Others in the hallway can also overhear the conversation.	**Which statements, if any, are accurate in describing the situation? Select the best response:** A. This is not a privacy problem because the information is not being recorded B. This is not a privacy problem because the individuals need the information to perform their duties C. Others in the hallway were witness to the incident D. It's just gossip E. None of the above
Q8	**MFOIPPA Requests** You are advised of an MFOIPPA request relating to your school. You ask staff to provide any records in their possession. A staff member approaches you to advise that there is a file with a number of records in it relating to the request. The file does not cast the school in a good light. The staff member asks if the file should be shredded. As the supervisor, which course of action should you take?	**Select the best response:** A. Shred it as long as it does not contain any personal information B. Shred it even if it does contain personal information C. Collect the file and provide all records to the MFOIPPA coordinator D. None of the above

Q1. Correct answer: Yes. Any unauthorized sharing of personal information is a privacy breach and must be reported.

Q2. Correct answer: You should consider all of the above options in response to the theft and privacy breach.

Q3. Correct answer: B is not true. Privacy requires security but security does not necessarily require privacy.

Q4. Correct answer: A, B and D are all examples of personal information that identifies an individual. C is not and E is not unless coupled with another piece of identifying information.

Q5. Correct answer: E. It is appropriate to speak to a colleague about the nature of the learning issues in order to help develop strategies to support student learning. Ideally this can be done by describing the learning issues, and key facts without oversharing personal information. In some circumstances the child's name may be known to colleague, and key factors of educational history may be relevant. However, C,D and G are not necessary for a general discussion about learning strategies.

Q6. Correct answer: A, B, C, and D are all required on a notice of collection. Always ensure this is on any form you create.

Q7. Correct answer: E. This is a privacy problem. Staff can only share PI where it is necessary and proper to do so – not in public places – and only with the employees who need the information to perform their duties.

Q8. Correct answer: C. The best course of action is to provide all records to the MFOIPPA coordinator as required by the legislation.

List of Educator Resources about Privacy

Privacy Tips Poster (5 Ways to Protect Your Privacy Online) — *https://goo.gl/52cdPm*

This eye-catching poster aimed at youth in grades 4–6 for classroom use. It offers tips for protecting personal information online to help equip students with the knowledge needed to make sound privacy decisions.

The poster is downloadable so it can be reproduced by educators and parents. However, you can also request copies for your library or classroom by emailing us at *youth-jeunes@priv.gc.ca*.

Social Smarts: Privacy, the Internet and You

The Office of the Privacy Commissioner of Canada has created a 12 page graphic novel, for tweens and younger teens to better understand and navigate privacy issues in the online world. There is a discussion guide (*https://goo.gl/Q5nzEf*) that educators can use to generate further discussion and learning. Download the novel or request copies of Social Smarts for your library or classroom by emailing *youth-jeunes@priv.gc.ca*.

Social Smarts graphic novel (PDF version) — *https://goo.gl/UR2LbU*

Social Smarts graphic novel (text only version) — *https://goo.gl/tr3N1q*

Know the Deal: The Value of Privacy Lesson Plan — Grades 6–8 (60–90 Minutes) — *https://goo.gl/tLt9Pm*

In this lesson, students are introduced to the idea that privacy is a fundamental human right and that their personal information is valuable. The lesson focuses on the "economics" of personal information and that most "free" apps and online services make some or all of their revenue by collecting (and in some cases reselling) users' personal information. Students will watch a video that illustrates the idea that they may be paying with their privacy and then discuss some of the ramifications of this. They will learn about tools and techniques for minimizing the personal information they share and create a public service announcement that helps them and their peers "know the deal" about the value of privacy.

Getting the Toothpaste Back into the Tube Lesson Plan — Grades 6–8 (2–4 hours) — ***https://goo.gl/At1F7w***

In this lesson, students watch a short video that compares getting rid of personal information online to getting toothpaste back into a tube. After a short discussion of how visual analogies like this work, students discuss the meaning of the video (that information online is permanent). They then read a series of short scenarios that help them identify four further principles of information online: that it can be copied, that it can be seen by unintended audiences, that it can be seen by larger audiences than intended, and that it becomes searchable. Finally, students create a simple animation that illustrates one of these principles.

Privacy Rights of Children and Teens Lesson Plan — Grades 9–12 (1.5–2 hours) — *https://goo.gl/mMkrDi*

In this lesson, students are introduced to the privacy principles that inform the Alberta and BC Personal Information Protection Acts, Québec's An Act Respecting the Protection of Personal Information in the Private Sector and the federal Personal Information Protection and Electronic Documents Act (PIPEDA) relating to personal information collection online. They learn ways to find out what personal information may or has been collected by platforms that they use, how to limit data collection about themselves, and the various forms of recourse that are available to them if they feel an organization is not respecting their rights.

Online Educational Services — What Educators Need to Know — *https://goo.gl/QiZ3A9*

A guide by the Information and Privacy Commission which explains the privacy risks of using online tools and services. There are many types of online educational apps, and their terms and conditions and privacy policies can vary. In many cases, the complexity of the terms of service and privacy policies may make it difficult to determine if the personal information of students will be collected, used, and disclosed in compliance with MFIPPA. This guide has some examples of practices associated with some online educational services to watch out for.

Think Before You Click Poster — *https://goo.gl/XPo4uz*

MEDIA SMARTS Digital Literacy 101 — Educator Resources

MediaSmarts has a range of resources to support teachers in implementing digital literacy into their teaching practice and to help them to develop digital literacy lessons and activities that suit their students' needs.

Digital Literacy Training Workshops

The *Digital Literacy Training Program for Canadian Educators workshop* provides an overview of essential digital literacy skills and key concepts of media and digital literacy, familiarizes participants with the digital experiences of Canadian youth, and introduces the resources and tools that are available through MediaSmarts' *USE, UNDERSTAND & CREATE* (*https://goo.gl/2LPgek*) digital literacy framework.

Each workshop is available as a self-directed tutorial or as a downloadable PowerPoint presentation ideal for presenting to a group. The workshop is timed to take three hours if all of the activities are included. If the activities are abridged or conducted by the facilitator it can be reduced to roughly two hours.

Grades K–12: Self-directed tutorial
https://goo.gl/QbxFGS (HTML5)
https://goo.gl/JMxVb2 (PowerPoint slide presentation in .zip format)

Grades K–6: Self-directed tutorial
https://goo.gl/ihWvMz (HTML5)
https://goo.gl/zKyagL (PowerPoint slide presentation in .zip format)

Grades 7–12: Self-directed tutorial
https://goo.gl/RA6DEF (HTML5)
https://goo.gl/cDHW9T (PowerPoint slide presentation in .zip format)

Instructions for Conducting a Workshop — *https://goo.gl/7Vzh5A*

Implementing Digital Literacy in the Classroom Guide
This Classroom Guide (*https://goo.gl/SzS4mw*)provides practical tools to help K–12 teachers make digital literacy a part of their classroom practice. While the training workshops focus on the five key concepts of digital literacy, this implementation guide looks at the specific skill areas identified as being essential for students to learn by the end of their secondary education: *ethics and empathy, privacy and security, community engagement, digital health, consumer awareness, finding and verifying and making and remixing*. The guide also addresses common challenges to integrating digital literacy into the classroom, such as limitations on available technology and classroom management concerns, and includes links to relevant MediaSmarts' and other resources, and apps and tools for creating digital media in your classroom.