

2017 GPEN Sweep Report

Online Educational Services



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Acknowledgements

The IPC is grateful to staff at the Office of the Privacy Commissioner of Canada who reviewed a draft version of this report and provided helpful comments. The IPC also wishes to express appreciation to the many volunteers who helped carry out the Sweep, including educators from the Ontario English Catholic Teachers Association.

CONTENTS

INTRODUCTION.....	1	Mobile apps	4
THE GPEN “SWEEP”	1	Social login	5
SWEEP METHODOLOGY	2	Internet tracking cookies	5
THE FINDINGS.....	2	3. PRIVACY POLICIES AND TERMS OF SERVICE	5
1. COLLECTION OF PERSONAL INFORMATION	3	4. DELETION OF PERSONAL INFORMATION	6
Creating accounts	3	Deleting student accounts.....	6
User profiles	3	Deleting educator accounts.....	7
2. COLLECTION, USE AND DISCLOSURE	4	IMPLICATIONS AND BEST PRACTICES FOR SCHOOL BOARDS AND EDUCATORS	7
Default settings	4	RESOURCES:.....	9

INTRODUCTION

There is a growing trend for Ontario educators to use technology and online educational services, such as digital learning resources, software applications, and internet-based teaching platforms, in the classroom. While these services may be innovative, accessible, and available at little or no cost, using them could put students' and parents' privacy at risk.

Under the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, which regulates the collection, use and disclosure of personal information, Ontario school boards are accountable for the information management practices of their educators. The Information and Privacy Commissioner of Ontario (IPC) oversees *MFIPPA* and has been actively engaged in raising awareness with boards and educators about the privacy risks of online educational services.

Last year, we worked with the Ontario Association of School Business Officials to develop a brochure-style information handout about the privacy risks of using some online services in the classroom.¹ We recommended that educators exercise caution before agreeing to use online educational services on behalf of their students and school boards. Today, we continue our efforts to ensure that Ontario school boards comply with Ontario's privacy laws.

THE GPEN "SWEEP"

The Global Privacy Enforcement Network (GPEN) was established in 2010 to foster cross-border cooperation among privacy regulators. The network is composed of over 60 privacy enforcement authorities in 39 jurisdictions around the world. Its members seek to work together to strengthen personal privacy protections in an increasingly global context. The IPC is a GPEN member.

Each spring, as part of the annual GPEN "Sweep," GPEN members conduct a coordinated review of the privacy risks of websites and mobile applications ("apps"). The IPC participated in the 2016 GPEN Sweep when we reviewed eight health care apps under the broad theme of "Internet of Things."

This year, the 2017 GPEN Sweep theme was "user control over personal information." The IPC worked with the Office of the Privacy Commissioner of Canada (OPC) to design and carry out a review of online educational services. We wanted to understand the transparency practices of these services (that is, whether they inform educators and students how they collect, use and disclose personal information), and how much effective control educators and students can exercise over their information that is collected, used and disclosed by the service provider and third parties. This Sweep report summarizes the findings of our review.

SWEEP METHODOLOGY

It is important to note that the Sweep is not an investigation or audit. It is a non-scientific survey designed to identify potential areas of concern or trends that might guide future outreach, collaboration and education efforts by privacy regulators. We do not name the services that we reviewed.

1 IPC, "Online Educational Services: What Teachers Need to Know" (Nov 2016)

To conduct the Sweep, we consulted with Ontario educators and school board staff to identify online services being used by educators in Ontario. We compiled a list of 40 web-based services where students could create accounts and online content, and communicate and collaborate with their educators, classmates and others online. We included some French-language and elementary school-oriented services.

We decided **not** to review online services or specific features that:

- were not available free of charge or on a trial basis
- required installing software, such as on a mobile device
- required users to access them via “social login,” or
- were currently being used by Ontario school boards pursuant to terms of service agreements between the service provider and the boards.

In the end, we reviewed more than two dozen online educational services. To carry out the Sweep, the IPC created fictitious student and educator accounts for each service. We noted how the services collected, used and disclosed personal information, what notices were provided to users, and what options users had to control their personal information.

The IPC and OPC divided the Sweep tasks. The OPC focused more on creating and using accounts, while the IPC focused on the ability of educators and students to delete their personal information and to close their accounts. In practice, there was considerable overlap in work between the two offices.

THE FINDINGS

As noted above, the following observations are general in nature. They are intended to raise awareness, inform understanding and stimulate discussions about the privacy risks of using online educational services.

Our findings are grouped into four categories:

1. collection of personal information
2. collection, use and disclosure
3. privacy policies and terms of service
4. deletion of personal information

1. COLLECTION OF PERSONAL INFORMATION

We examined the collection practices of over two dozen online educational services. Overall, most services appeared to limit the collection of personal information provided directly by users.

CREATING ACCOUNTS

In almost all cases, educators had to provide their name and email address to create an account. Sometimes they were invited to provide the name of their school but in most cases this was not required.

Most, but not all online services also required students to create accounts the same way by providing their name and email address. For online services targeted at pre-teens, their age and a parent/guardian's email address was also required.

Roughly a third of the online services allowed educators to act as administrators and to create "virtual" classrooms or online spaces, which students could access by inputting a special code given to them by their classroom educator. The access code could be the same for all students, or be uniquely created by the educator for each individual student (see discussion below under "User Profiles"). In both scenarios, students did not need to create accounts or provide their own personal information, such as names and email addresses.

USER PROFILES

Creating an account results in a user profile, which students could often modify. For example, students could choose a different username or add a profile image. A few sites allowed, but did not require, students to add additional biographical information and instant messaging identities without explaining why. However, in general, most services that we reviewed limited the ability of users to add personal information to their profiles. A substantial number of services discouraged students from using full or real names.

As noted above, several online services allowed educators to act as administrators by creating and adding student profiles to their virtual classrooms, effectively deciding how identifiable the students are to the online service. Several online services advised educators to minimize personal information used to create a profile by assigning pseudonyms to students. Students could then access their profiles by inputting a unique access code provided to them. In this way, students did not need to provide their personal information and could use the service in a pseudonymous manner.

2. COLLECTION, USE AND DISCLOSURE

DEFAULT SETTINGS


Once created, accounts and profiles allow students to participate in online spaces and activities, and to create new identifiable content. Most online services restricted the public visibility of students' profiles, contact information, and their online activities by default, effectively limiting the ability of others to collect, use and further disclose the students' personal information.

However, by default, online educational services have access to all the personal information generated by users and retained on the providers' servers. We did not classify the other types of personal information collected, used and disclosed because these varied among service providers

and the intended purpose(s). For example, details of students' online activities might be recorded by the educational service provider in order to provide educators with insights about students, such as time taken to complete an assignment.

In keeping with the Sweep theme, we want to flag some notable collection, use and disclosure practices that we observed which may be less than transparent to users and effectively limit their ability to exercise control over their personal information.

In our survey, we noted, but did not test, three common scenarios where collection, use and disclosure of personal information was possible: through the use of mobile apps, social login, and browser tracking cookies.



Online services may collect and disclose students' personal information through the use of mobile apps, social login features, and browser tracking cookies.

MOBILE APPS

Nearly half of the online educational services we surveyed were also available in mobile app form, which must be downloaded, installed and configured on computing devices (which the student may or may not own). Apps may offer different functionalities and request access to personal information stored on the device, such as device identifiers, cell numbers or location data. Depending on how software apps are designed, installed and configured, students may unwittingly allow the collection of new or different personal information². Consequently, there may be new and different privacy risks associated with using mobile apps.

SOCIAL LOGIN

A third of the online educational services offered students the option to register and access using third-party "social login" or "social sign-in" providers. Facebook Connect and Google+, for example, offer the convenience of using a single login "identity" across the web. Users do not need to create or remember new usernames and passwords because they can rely upon their social login "identity providers."

However, the convenience of social login depends on data-sharing technologies between the social login "identity provider" and the online educational service. Implemented poorly, social login can result in excessive collection and disclosure of detailed profile and other identifiable information between the two sites. Use of social login may limit students' ability to prevent the tracking of their online activities across the web. Consequently, there may be new and different privacy risks associated with the use of social login.

² See Serge Edelman, "We tested apps for children. Half failed to protect their data," *Washington Post*, July 27, 2017

INTERNET TRACKING COOKIES

Tracking cookies are small plain text files that are saved to and from a user’s browser while they are surfing the web. They are used to personalize the browsing experience by tracking and storing a user’s activities and preferences. *Third-party* cookies are cookies that are set by internet servers other than the online educational service being visited. Their presence allows additional parties to track users’ activities on the site and to correlate them with users’ activities elsewhere on the web. Third-party cookies enable the collection and use of personal information by third parties, such as data analytics firms and advertisers.

Nearly all online educational services that we surveyed attempted to set third-party cookies in our browsers upon access and use of their site. Third-party cookies represent a privacy risk if their use is associated with an individually identifiable person. Most site privacy policies disclose the presence and use of third-party cookies but do not provide specific instructions or meaningful options for preventing or managing them. We were able to block all third-party cookies in the services reviewed with no apparent loss of functionality. However, many educators and students may not know how to do this.

Most privacy policies disclosed the presence and use of third-party cookies but do not provide details or meaningful options to block or manage them.

3. PRIVACY POLICIES AND TERMS OF SERVICE

Privacy policies inform users how the website, service or app will collect, use and disclose their personal information —and what options users may have in this respect. In addition, terms of service³ specify the conditions users must agree to when using the website, service or app. Both documents should be read and understood by educators and students, where appropriate, prior to using the service.

Every online educational service that we surveyed posted a privacy policy and terms of service that was generally easy to find. We noted that they were lengthy documents that would require considerable time for students—especially younger students—to read and to understand.

Privacy policies and terms of service were lengthy documents that could require considerable time for students to read and to understand.

We also noted that links to privacy policies and terms of service were often absent or hard to find once the account had been created. This means an educator or student cannot easily refer back to the policies and terms of use once they have clicked “I Agree.”

Privacy policies and terms of service could be hard to find after signing up and when using the services.

3 Alternatively called “terms of use” or “acceptable use agreement.”

4. DELETION OF PERSONAL INFORMATION

In general, the online educational services that we surveyed enabled students to permanently close their accounts and to delete their personal information, unless those accounts were created by their educators. However, there were some notable exceptions, discussed below. In addition, the ability to delete online content differed between students and educators.

Where students created accounts themselves, rather than being assigned accounts, all the services that we surveyed provided instructions to students on how to change or remove their online content. However, sometimes those instructions were unclear or hard to find.

Instructions on how to delete online accounts and personal information were sometimes unclear or hard to find.

An important exception to students' ability to delete their personal information in accounts they created themselves occurred in those online services where educators had administrative rights. In at least two instances, educators were able to retain access to copies of the student's work even if it had been deleted by the student. This means that students' online work would be retained and potentially accessible not just to the educator but to the online service, despite being "deleted."

DELETING STUDENT ACCOUNTS

All the online educational services that we surveyed provided instructions on how to close an account. Students were generally able to close their accounts by navigating through a series of warnings and alerts. Doing so typically meant deleting or losing access to all personal information associated with the account. As noted above, an important exception to this ability occurred in a third of the services surveyed where educators had full administrative control over the accounts.

A minority of online services imposed delays on deleting accounts and online information to give students (and parents) the opportunity to download (or print) their online content.

Less than half of the online services provided readily available information about their retention practices, and only a quarter of the sites deleted dormant or inactive accounts within one to two years.

A majority of the online educational services did not have a policy on deleting dormant or inactive accounts.

DELETING EDUCATOR ACCOUNTS

Educators faced similar scenarios as students when deleting online content and closing their accounts. Most if not all services provided instructions on how to do so, but educators had important additional restrictions not faced by students.

Unlike student accounts, we were surprised to find that many online educational services do not allow educators to delete their virtual classrooms, accounts and online contents (including student information) but must, instead, *archive* them for a period of one to two years or longer. We found

the archive feature to be somewhat opaque because it was unclear to us how the information might be retrieved or used by the service provider once the account is archived.

Some online educational services continued to have access to students' personal information even after deleted by the student.

Also unlike student accounts, a significant percentage of these educators' accounts required their owners to request, in writing, that the online educational service delete their accounts on their behalf rather than being able to do it themselves.

IMPLICATIONS AND BEST PRACTICES FOR SCHOOL BOARDS AND EDUCATORS

As noted above, Ontario school boards are accountable for the information practices of their educators and must ensure that these practices are in compliance with *MFIPPA*.

The ability of educators and students to control the collection, use and disclosure of student personal information when using free online educational services is essential to ensure students' privacy, and also for compliance with Ontario's privacy and access to information laws.

In Ontario, educators have some discretion to achieve pedagogical goals in innovative and cost-effective ways, but when signing up for free online educational services, they may be agreeing to practices that are inconsistent with their school or school boards' policies and not compliant with *MFIPPA*.

When signing up on behalf of their students, educators may be agreeing to information management practices by educational service providers that are inconsistent with their school boards' policies and not compliant with *Municipal Freedom of Information and Protection of Privacy Act*.

The results of our review are consistent with similar studies and advice offered elsewhere.⁴

In light of these observations, we recommend that educators considering the use of free online educational services:

1. **Consult with the school board, principal and/or administrators** before selecting an online education service. The Ministry of Education and many school boards have evaluated and reviewed online educational services and maintain a list of those approved for use in classrooms. Schools may also have already purchased similar software for use on school-owned computers. School boards, principals and administrators can also help educators to understand relevant requirements under the *Education Act*, *Ontario College of Teachers Act*, and related professional standards.

4 For example, see: U.S. Department of Education, Privacy Technical Assistance Center, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices," (Feb 2014); Common Sense Education, *Privacy Initiative: Privacy Evaluations for EdTech Products*; and Mary Jo Madda, "Why Schools Should Be Wary of Free Tech Products—And Startups Shouldn't Make Them," *Forbes* (July 28, 2017)

2. **Read the privacy policies and terms of service** to understand what personal information about students may be collected, used and disclosed by the online educational service. Pay special attention to any uses and disclosures that involve third parties. Where appropriate, consult with parents/guardians and consider offering students the ability to opt-out and/or to use alternative tools and services.
- 3 **Minimize the identifiability of students and the collection of their personal information** by the online educational service, where feasible. Use services which do not require students to identify themselves by disclosing their name and email addresses or other identifying information, or assign students a pseudonym or fictitious name.
4. **Seek the involvement and express consent of parents and guardians, where appropriate.**

Online educational services may allow parents to view, participate in, or exercise control over their child’s online activities. Depending on circumstances, educators may need express consent prior to disclosing personal information about students to a publicly-accessible site, or to the online service provider for inconsistent purposes, such as marketing.

5. **Provide timely and ongoing guidance to students** on appropriate uses of online educational services. This may include advice on how to:
 - create an online account
 - create a user profile
 - create or upload online content
 - configure account settings and preferences
 - manage cookies, especially “third-party” tracking cookies
 - download and install software, especially on personal computing devices
 - use social logins safely
 - delete online content
 - close accounts

For further information about privacy and online educational services and the work of the IPC, see the resources listed on the next page.

RESOURCES:

Office of the Information and Privacy Commissioner of Ontario

- *Ontario’s Municipal Freedom of Information and Protection of Privacy Act: A Mini Guide*
<https://www.ipc.on.ca/wp-content/uploads/Resources/municipal%20guide-e.pdf>
- *Online Educational Services: What Educators Need to Know* (2016)
<https://www.ipc.on.ca/privacy/data-and-technology-management/oes/>

- *Online Privacy: Make Youth Awareness and Education a Priority* (2009)
<https://www.ipc.on.ca/wp-content/uploads/Resources/youthonline.pdf>
- *A Guide to Ontario Legislation Covering the Release of Students' Personal Information* (2011),
<https://www.ipc.on.ca/wp-content/uploads/2003/07/educate-e.pdf>
- *Thinking About Clouds? Privacy, security and compliance considerations for Ontario public sector institutions* (2016)
<https://www.ipc.on.ca/wp-content/uploads/2016/08/Thinking-About-Clouds-1.pdf>

IPC and Toronto District School Board, *F.A.Q. – Access and Privacy in the School System: A Resource for Parents, Teachers, and Administrators* (2012) <https://www.ipc.on.ca/wp-content/uploads/Resources/faq-e.pdf>

IPC, Upper Grand District School Board, and Peterborough, Victoria, Northumberland and Clarington Catholic District School Board, *Posting Information on Websites: Best Practices for Schools and School Boards* (2003), <https://www.ipc.on.ca/wp-content/uploads/Resources/bp-sch-e.pdf>

OTHER RESOURCES

Ontario Ministry of Education, Ontario Software Acquisition Program Advisory Committee (OSAPAC), *Licensed Digital Learning Resources*, <https://www.osapac.ca/dlr/>

Ontario Association of School Business Officials (OASBO), Information Management/Privacy & Access Committee, www.oasbo.org/?page=IMPACCtee

Ontario Privacy and Information Management (PIM) Taskforce, <https://www.pimedu.org/>

PIM Toolkit: <https://www.pimedu.org/files/toolkit/PIMtoolkit.pdf>

Webcast: Understanding Privacy Considerations: <https://www.pimedu.org/videosboardstaff.html>

U.S. Department of Education, Privacy Technical Assistance Center

- *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (2014)
<http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf>
- *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service* (2015), http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf

Common Sense Education, Privacy Initiative: *Privacy Evaluations for EdTech Products*, <https://www.commonsense.org/education/privacy>

Electronic Frontier Foundation, *Spying on Students: School-Issued Devices and Student Privacy* (2017), <https://www.eff.org/wp/school-issued-devices-and-student-privacy>

MediaSmarts and Canadian Teachers' Federation, *Young Canadians in a Wired World, Phase III: Connected to Learn, Teachers' Experiences with Networked Technologies in the Classroom* (2016),

<http://mediasmarts.ca/research-policy/young-canadians-wired-world-phase-iii-connected-learn>

MediaSmarts, *Click If You Agree: Understanding Online Terms of Use and Privacy Policies in Plain Language – Teachers' Guide* (2016) <http://mediasmarts.ca/sites/mediasmarts/files/pdfs/backgrounders/click-if-you-agree-guide.pdf>

Office of the Privacy Commissioner of Canada,

- *Collecting from kids? Ten tips for services aimed at children and youth* (2015), https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/02_05_d_62_tips/
- *What kind of information is being collected about me when I'm online?* (2012) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/fs-fi/choice-choix/>

2017 GPEN
Sweep Report
Online Educational
Services



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

October 2017