OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

FIPPA and online learning during the COVID-19 pandemic

APRIL 2020

This document provides recommended guidance for educators to help them choose online learning tools that comply with the requirements of BC's *Freedom of Information and Protection of Privacy Act* (FIPPA). It includes information about recent, temporary changes to FIPPA in response to the COVID-19 crisis that allow for the use of tools that store information outside of Canada.

Research before you start using a product

FIPPA requires public bodies to ensure personal information is secure. To meet this requirement, research the product you intend to use. Determine what the company offering the product does with the information you, or your students provide it. Seek an understanding of how the company protects that information from risks like unauthorized access. Start by visiting the product's website and read the "about us" and the "privacy" section. Next, use a search engine to type in the product's name and the word "privacy" or "security" or both. Look for any articles or information from reputable sources about the product's privacy and security settings. If the company does collect information, determine how it is being used.

Reach out to IT staff in your organization, as they may have information about the product you intend to use. Where possible, work with qualified privacy and technology professionals experienced at protecting data in systems.

In the end, you should be able to learn basic information such as the name of the company behind the product, whether they provide reliable contact information in the event you have questions, and what the product's general privacy and user terms are. If you cannot get this information, do not use the product because you do not have enough information to know whether it complies with the security requirements of FIPPA.

Determine how the company makes money

What is the company's business model? Do you pay them for a service? Is it free? If it is free, then the company likely makes money from the information that you and your students enter into the tool. The company might "data mine" that information for itself, or it might bundle it up and sell it to other companies. Note that even companies that charge a fee to use a service

might also use the information that educators, parents and students enter into it. Other companies might offer low introductory rates and then increase fees once it has users' data and it is more difficult to switch services. This is why researching the product ahead of time is so important.

Investigate where the company is headquartered

The EU has much stronger privacy laws and oversight than most of the United States. California has a new strong privacy law, but that law only applies to residents of that state, so Canadians cannot rely on it to protect them. Canada's privacy laws offer protections that are somewhere between the EU and the US. Look for companies that are headquartered in countries with strong privacy laws. Avoid using products owned by companies in countries that do not have democratically-elected governments and independent courts. These companies may promise high privacy and security standards, but typically have inadequate or no enforcement mechanisms in place to ensure they keep their promises.

Identify where the data is stored

A company headquartered in one country might store data in several other countries. Before you use an online tool or service, find out all the countries in which they store their data. Where possible find out the locations of production servers, data backups, and disaster recovery. If the company won't tell you in what countries its servers are located, do not do business with them.

Storing information outside of Canada

Before the COVID-19 crisis, educators had to get the consent of students, teachers and others to use tools that store personal information outside of Canada. The BC government recently issued Ministerial Order 085 (MO85) allowing public bodies to store information outside of Canada without consent under specific conditions set out in the order. The order is intended to enable public bodies to continue operations through greater use of third-party tools and applications during the state of emergency. This means that an educator does not require a student or parent to consent to use an online platform.

Under the terms of MO85, a public body must be able to demonstrate that using the online tool is necessary for maintaining programs or services during the COVID-19 crisis, such as providing distance learning and collaboration. Additionally, the public body must ensure that they take all reasonable steps to delete the information from outside Canada once they are done with it. For this reason, educators should check in advance to make sure the online tool or service lets them delete the information they enter into the tool. If it does not, then the educator should either not use the product, or they should ask individuals for their consent to store information outside of Canada.

Importantly, whether an educator seeks consent to store information outside of Canada or not, the requirement in FIPPA to protect personal information from unauthorized access and other

risks still applies. For that reason, do not use services offered by companies if you do not have a good understanding of what they are doing with your information or where in the world they are keeping it. Do not use products that have been found by regulatory authorities to be guilty of privacy or security breaches. Often, you can learn if a product has privacy issues or a company has privacy compliance issues by speaking with an IT professional or by researching reliable sites online.

Look into security settings

Anyone using an online service or making it available to staff should locate the security settings and should, where possible, set the default setting to the highest level of security. In the event security settings are left to the user, they should be clearly instructed to do the same. For example, many videoconferencing platforms offer end-to-end encryption, but you have to turn it on. Other websites use all kinds of tracking features, but you can turn them off by accessing your profile settings. Almost always, the user must turn these features on, because they are not the default setting.

Avoid oversharing

When using a technology platform, disclose as little personal information as possible. Avoid the use of unique identifiers like student numbers, date of birth, home address, telephone number, or anything else that can be matched with other information that identifies who an individual is Where possible, use pseudonyms, or first names only.

You should not disclose sensitive information such as custody arrangements, sensitive health issues or financial information on free online products. Prohibit your students and parents from doing the same when they are using online tools under your direction for online learning purposes. Additionally, avoid hitting the “recording” feature for online video and audio sessions unless there is an operational need to do so.

Avoid the “easy” option

Although it may be tempting to employ easy to use free products that educators are familiar with in their personal lives, they should carefully assess whether those same products are suitable for online learning. Just because it the easiest or the most familiar to use doesn’t make it compliant with FIPPA.

Use work email and secure file transfer on your local area network when possible

Sometimes, it may be easier to communicate directly with parents using an email list from your work email account. Alternatively, you can ask your IT staff to set up a secure file transfer site to deliver and receive class materials. Another option is to ask your organization to purchase software that it can install on its own servers and provide you and your students with access to. These solutions are all more secure because your employer, and not a third company, is in control of the data and how it gets used.

Focused Education Resources has developed template privacy impact assessments for many online learning platforms. They are available to members on their website.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.