Maintaining Privacy of Personal Information While Using Web Technologies

Protecting the Privacy of Student Data: Required Actions for Compliance with BC's FIPPA Law

British Columbia (BC) has one of the strictest privacy laws of personal data in North America. It exists to ensure BC citizens are protected when it comes to storage and access of personal identifiable information. The General Data Protection Regulation (GDPR) which came into effect in May of 2016 is another example of a strict privacy regulation on data protection and privacy for the European Union (EU) and the transfer of data outside of the EU.

To abide by BC's Freedom of Information and Privacy Protection Act (FIPPA) Regulation, faculty members must deploy **three principles when in situations about privacy of student information:**

1) give **notice** to students when they are sending/requiring them to send their data to a location outside of Canada

2) provide **knowledge** of why they are doing this, and if required

3) obtain **written** consent from students for doing so. You can apply these principles to almost any privacy situation to show you have done your due diligence.

Written consent is the highest level of 'due diligence' when classroom work requires the use of social media, or when a faculty member or student forwards email to Gmail/Hotmail (web email services), and when a course requires the use of online textbooks or textbook websites for doing activities and testing of knowledge.

Educating students is an important part of maintaining their privacy.

It is the responsibility of individual faculty members to ensure that they are compliant with FIPPA regulations. The following information is provided to help ensure that faculty members are aware of their responsibilities.

When to Think About FIPPA

Any time students' personal, identifiable information (first name, last name, date of birth, course student is enrolled in, student grades, home address, student Institutional ID) is stored on a server outside of Canada, or the parent company that owns the server is located outside of Canada, students must be provided with notice, knowledge, and consent. Personal, identifiable information includes any information that can be used to identify an individual student including photographs, file names of documents, student assignment titles, videos, audio files etc. See Guide to Access and Privacy Protection under FIPPA and Privacy Guide for Faculty Using 3rd Party Web Technology (Social Media) in Public Post-Secondary Courses

Instructor Emails

Any email that contains student's personal, identifiable information should **ONLY** be accessed from **Canadian-based services**, such as NIC Outlook email account (hosted at NIC). Services such as Gmail, Hotmail, Yahoo, etc., host their services outside of Canada (on servers around the world), and **should not be used to access emails** that contain student personal identifiable information (including accessing NIC webmail from a public computer in another country). This would be a violation of the FIPPA regulation.

Online Textbook Resources

Any online learning resource, such as textbooks or any supporting materials included in textbooks (labs, quizzes, resources to access), that faculty require students to use should only be hosted in Canada. If the resource is located outside of Canada, or the parent company is located outside of Canada, faculty must ensure they give students notice of information that will be stored outside of Canada, knowledge of why they need to access the site, and ensures there is **student consent** (written or some alternative form of recording consent). In this way, students are made aware of the implications of having their data reside outside of Canada and what other companies can do with their data.

Social Media, Web Tools and Online Technology Used in the Classroom

Many students access social media and various web tools outside of the classroom. What students do with social media outside of the classroom on their own is their business, and not the responsibility of faculty. If students are **required to use social media, web tools or online technology resources** as part of their classes (make a Prezi, post to Twitter, create a Facebook account, upload video to YouTube, respond to a survey with personal data etc.), and that tool is based outside of Canada (which almost every company is), faculty are responsible to ensure they give students **notice** of information that will be stored outside of Canada, **knowledge** of why they need to access the tool and how it is impacted by BC FIPPA laws, and capture **student consent** (written or some digital form of recording consent that the instructor keeps for up to 2 years).

Obtaining Student Consent

1. Look at the fine print for the resource, activity or website you are requiring students to use in their classes (remember if it is an optional assignment/activity and they can use other tools not hosted online outside of Canada - you are fine). Read the privacy policy: what data does the resource capture? where does the data live? what alternatives are there? how much data is required to be captured?

2. Once you have all the information, create a consent form for your students. A consent form is required **FOR EACH COURSE** clearly outlining the assignments, activities and required learning that makes use of a tool or resource that is putting student information on servers outside of Canada.
    - Unfortunately, you cannot have a 'blanket' program or degree consent form. You need the details for each course assignment/activity spelled out on its own consent form.

3. **There is sample NIC Consent Form** for an Online Textbook Site for you to acquire from the Centre for Teaching and Learning Innovation, edit and use with students. Ensure you remove all *'sample'* content and insert your own information. There is also a **blank NIC Consent Form** for anything other than online textbooks that require student consent.

4. You are also able to create a 'digital consent form' through an online content page in Blackboard Learn where students read and select their response to a question (consent) so you have record of their consent/non consent. Consider using a survey or test on the first page with no marks to record responses to a consent question in Blackboard.

5. If you wish some assistance to proofread your consent form or you have questions, kindly email the Centre for Teaching and Learning Innovation CTLI@nic.bc.ca for assistance.

Alternatives to Student Consent

1. Research the technology and your assignment/task to ascertain if your students/you require the collection, upload, and use of personal identifiable information (often you may not and can use the social media or web tool without needing such information). You may be able to have students skip sections intended to capture personal identifiable information.

2. If you or the web tool requires personal identifiable information – find out how much your students really need to supply (or are connected to through accounts) and what are the privacy risks or abilities to make more private information – then use a consent form.

3. If a student refuses consent – have a Plan B. Some students, who do not want to engage in privacy-laden activities, should have an alternative that fulfils a lot of the main learning intentions, but doesn't expose them to privacy risks (e.g., use learning management system – Blackboard Learn etc.)

4. Inquire about 'on site' or 'Canadian-hosted' tools that may allow you to do similar activities but not have to use US servers for storage, hosting, and access.

5. Educate students – let them know what is going on. They may have some solutions!

6. Try using pseudonyms for some social media elements that will not expose personal identifiable information.

Adapted from orginal version from Vancouver Island University written by L. Knaack and other members of the Centre for Innovation and Excellence in Learning