BC Privacy and Security in Post-Secondary Education - Considerations[i]

The BC Privacy and Security in PSE Group is a grass roots collection of individuals from teaching and learning or educational technology centers from various post-secondary institutions in BC. This group is in the process of identifying promising practices, useful tools, policies and processes that enable instructors to either adopt technology or approach their privacy office and/or CIO office with an informed request to use the appropriate technology for their classes. One of the starting points is to use the fippa.bccampus.ca as a repository for resources and information that will assist instructors. This same site may also be a repository for resources and information to be shared among privacy officers and CIOs. We are in the early stages of development and encourage input for content and discussion from interested faculty in BC.

In the meantime, how do you approach adopting educational technology tools with your course(s)? There are some basic assumptions and considerations for using educational technology in BC.

1. Check your institutions policies and procedures first. Start with the teaching and learning centre or educational technology centre at your institution. If you do not have these resources, then the next stop would be the Chief Information Officer (CIO) or Information Technology department at your institution. If there are policies in place that direct and prescribe how to adopt educational technology at your institution, it is important to keep your use of educational

technologies within the parameters set out by the institution. It is the institution that is liable for any privacy breach.

2. If you want to use tools that are already supported and endorsed by your institution, then the privacy and security needs have already been examined by the institution. For example, the LMS or video conferencing tools set up by the institution.
3. If you want to use educational technology tools that are not part of the institution's systems, and policy supports use of other tools, then these are some of the considerations you need to examine:
    a. Is the tool (social media, collaborative spaces, repositories, etc.) hosted in Canada by a Canadian company?
    b. Do the benefits of using the tool outweigh the risks associated with the use of the tool?
    c. Do you know what the risks are?
    d. Is there someone at your institution that can assist with evaluation of the tool?
    e. Can you use the tool in compliance with FIPPA?
    f. Does the use of the tool require personal information, e.g. student name, address, student id, and/or program?
    g. If the use of the tool collects personal information can you mitigate the risk by educating the students to not use their institutional data, e.g. student id, program, course, and/or location?

It gets very complicated if you decide to use educational technology tools that are owned or operated outside of Canada. It is really important to know if the data is stored within Canada, and if the data back up is within Canada. It is important to recognize that many companies use US cloud services to store and/or back up their data holdings. Once you have determined that there is a risk of the personal data being outside of Canada, you are obligated to get student consent for their use of the tool. Key factors in getting student consent:

- Informed consent
- List the personal data that will be collected
- Identify how the personal data will be used (for what purpose)
- Identify how the personal data will be retained (stored)
- Identify how long the personal data will be retained
- Identify the process for correcting the personal data
- Identify how the personal data will be disclosed (if at all)
- Provide an "out" for the student (an alternate method to participate)

It is often difficult to have this consent built into the account creation step of the tool so having students sign a hard copy consent form (where possible) or email their consent is required. The other option is to create a module in your course's LMS that informs the student of the risks and they can accept or decline using the tool.

Often students will already have personal accounts with social media and/or cloud services however, the obligation to protect their personal data moves to the institution if you require they use those same tools for your course. If students choose to use those same tools to collaborate on their own, without being required to by the instructor, the risk remains with the students.

Educating students on their digital footprint and how to create accounts in these tools will go along way in ensuring their online activities don't reveal third party personal information, do not use the same username and password, and don't disclose personal information that is not required for the tool(s). Building intelligence around examining end user licenses (many state the company can change the privacy policy without notice to the user) and terms and conditions of use for these tools will help support an informed choice.

In summary, the best tools to use with your class might be the tools that carry the biggest risk to a privacy breach. If you still want to use these tools, then due

diligence is required around where the data is stored, who can access the data (e.g. US Patriot Act http://en.wikipedia.org/wiki/Patriot_Act), how to minimize the amount of personal data that is shared, and ensuring informed consent is collected.

Resources:

Office of the CIO (government) has a number of templates and useful information that can be used by public bodies: BC OCIO. The OCIO has done some corporate PIAs for government use, but could be a good starting point for other public bodies to use.

- Training Presentation Slides: Freedom of Information and Protection of Privacy Act
- Twitter Checklist
- Blogger Checklist
- Single Purpose Consent Template

The Information and Privacy Commission (OIPC) website also as some resources that can assist with interpreting FIPPA.

- https://www.oipc.bc.ca/

There are some examples in the BC system for using consent forms, policies, and best practices. We also find resources from the K-12 sector that are helpful in the PSE sector. We have not curated these resources yet, but here are few links that you might find helpful:

- *VIU's Privacy Guide for Faculty Using 3rd Party Web Technology (Social Media) in Public Post-Secondary Courses*

- https://www.tru.ca/eureka/compliance.html
- http://opentextbc.ca/teachinginadigitalage/
- COTR Social Media Policy
- http://www.tonybates.ca/2011/03/25/cloud-based-educational-technology-and-privacy-a-canadian-perspective/
- https://storify.com/jhengstler/twitterview-and-chat-with-assistant-commissioner-m
- http://edmedia.tlc.sfu.ca/tlc-media-expo/edmedia-debate-webcast/
- https://jhengstler.wordpress.com/2014/04/24/the-compliance-continuum-fippa-bc-public-educators/

For information on the **BC Privacy in PSE Group** please contact

Denise Goudy, Manager, Collaborative Services

BCcampus, 778-679-2729 e: dgoudy@bccampus.ca

[i] The content in this document is based on preliminary discussion with the BC Privacy in PSE Group, experience with FIPPA through the OCIO and OIPC, and various projects facilitated by BCcampus. This content has been compiled for discussion purposes only.