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

A Vancouver Island University Publication
Produced with the Support of BCcampus

February 2011

Concept and Development:
Sheila Cooper, B.A., M.Ed. and Judy Southwell, M.A., Vancouver Island University

Researched & Written by:
Pamela Portal, B.A. LL.B., Privacy Consultant
privacyguide@shaw.ca

What This Guide Is and Who It Will Benefit

This privacy guide was developed specifically for use by faculty members of British Columbia's public post-secondary institutions. The guide:

- Sets out the main privacy principles and requirements of BC's *Freedom of Information and Protection of Privacy Act*;
- Explores the risks to privacy of using 3rd party web technology (social media) in post-secondary courses;
- Offers guidance on how to mitigate the privacy risks inherent to social media; and
- Provides sample privacy tools for protecting personal information online.

Due to the ever-evolving nature of computer technology and the wide range of educational methodologies and goals, it is not possible for this guide to cover the privacy risks inherent to all types of social media in all classroom situations. The guide does, however, provide important information about information privacy legislation governing faculty in BC's public post-secondary institutions and guidance on how to apply the law to the use of social media in programs and courses.

This guide is not a legal document and does not constitute legal advice.

Note: The terms 'class' and 'classroom' refer to face-to-face, online or hybrid learning environments in a post-secondary institution.

Format of the Guide

The guide is divided into four parts:

1) Introduction;
2) Five Fundamental Privacy Questions;
3) Conclusion; and
4) Appendices A, B, C and D (Appendix D revised January 2011).

The introduction provides background on information privacy laws in BC. The five privacy questions explain BC's *Freedom of Information and Protection of Privacy Act* and discuss its application to social media used in public post-secondary courses. Appendix A features a glossary of general privacy terms. Appendix B provides a sample student consent agreement form. Appendix C contains a sample user agreement form and Appendix D provides a privacy and technology tips sheet.

The Appendices have been designed to stand alone if need be. However, the remainder of this privacy guide is inter-related and ideally should be read and used together.

Introduction

Privacy is an elusive concept to many people. What one person considers private information, another may willingly share with a large circle of friends and even strangers. This is especially true in the age of **social media**[1] where information can be disclosed to millions of people instantly with the mere push of a button. Is this a good thing? The answer is both yes *and* no, depending on why and how information is shared.

While digital information-sharing provides countless opportunities for community-building, collaboration and education, broad disclosure of personal information for these or other reasons can have potentially damaging effects. At the very least, indiscriminate personal information-sharing may increase circulation of spam. More seriously, wide exchanges of personal information may cause some individuals loss of important health, educational, employment or financial benefits. At its most damaging, publication of personal information on the web can, and has, stigmatized vulnerable individuals, tarnished or destroyed reputations, terminated careers and even caused some individuals the loss of their jobs, families or identities.

Clearly, protecting privacy is a serious issue and should be considered carefully by those individuals, groups or organizations planning to use digital technology with the capacity for widespread distribution or storage of personal information. With this in mind, governments across Canada over the last decade have introduced or revised information privacy laws to ensure enhanced protection for personal information.[2]

In British Columbia, there are two main information privacy laws: the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). These laws set out the minimum standards that employers, employees and service providers must follow to prevent unreasonable, unnecessary or unsafe sharing of personal information belonging to staff, clients, customers and the general public. For public sector employers, employees and service providers in BC, which includes staff of publicly-funded educational institutions, the governing law is FIPPA.

---

[1] "Social media" are the web technology and tools used by individuals or groups for online, interactive sharing, exchange and collaboration of words, sounds and images for fun, business or social purposes. Some examples of well-known social media are Facebook (http://www.facebook.com), Twitter (http://www.twitter.com), YouTube (http://www.youtube.com) and Wikipedia (http://www.wikipedia.org).

[2] Canada is a leading country for privacy protection legislation and BC's privacy laws are arguably the strongest in Canada. Great Britain, Australia and New Zealand have similarly strong privacy legislation. The United States, however, has weaker and more selective protections, varying greatly by jurisdiction and sector.

Under FIPPA, all public post-secondary employers, employees and service providers have a responsibility to protect the privacy of personal information[3]. This requirement extends to all aspects of a faculty member's job, including the use of social media as a teaching aid. Since social media can be used to share information rapidly and widely and since FIPPA regulates how personal information may be shared, it is important for instructors in BC to understand FIPPA rules and how to apply them when using social media in class.

The primary questions typically asked by instructors are:

- What personal information can I collect, use or disclose when integrating social media as a teaching aid?
- What responsibility do I have for the protection of students' personal information when I require them to use social media to complete class assignments?
- Is there anything I can do to mitigate the privacy risks of using social media?
- Where can I go for more assistance?

The question and answer segment that follows addresses these issues in detail and offers practical step-by-step guidance and tools for protecting personal information and exercising due diligence under FIPPA when using social media for instructional purposes.

[3] "Personal information" is defined by FIPPA and explained in Question 1 below. See also the general definition of personal information set out in the glossary in Appendix A.

Five Fundamental Privacy Questions

There are five fundamental privacy questions in this section. Questions 1 and 2 discuss the specific duties and responsibilities instructors have for protecting personal information under FIPPA and the application of those rules to the use of social media in class. Question 3 presents practical steps that instructors can take to use social media in a privacy-sensitive manner. Question 4 provides some useful privacy tools for engaging social media in class and Question 5 offers additional sources of information and assistance.

QUESTION 1
What are my duties and responsibilities as an instructor under FIPPA regarding the privacy and protection of personal information?

Under FIPPA, instructors may collect, use, disclose or store personal information, but with certain restrictions. Protecting personal information is the key subject matter of the privacy provisions in FIPPA, so it is important to understand what "personal information" is and how it may be appropriately collected, used or disclosed under the law.

Definition of Personal Information in FIPPA

- **Personal information** is defined by FIPPA as recorded information about an identifiable individual other than contact information.[4]

- A **record** is anything on which information is recorded or stored by graphic, electronic, mechanical or other means, including documents, maps, photographs and digitally-captured information, sound or images.[5] Unrecorded verbal statements or exchanges are *not* covered by FIPPA.

- An **identifiable individual** is an individual who can be uniquely identified by one or more pieces of personal information, such as name, age, address, gender, physical attributes and health, educational or economic status.

- **Contact information** is the name, title, business telephone numbers, business address, business emails and business fax numbers enabling the individual to be contacted at his/her place of business. Thus, faculty members' names, office

[4] See also the general definition for personal information set out in the glossary in Appendix A.
[5] A "record" under FIPPA does not include a computer program or any other mechanism that produces records. See the general definition for record set out in the glossary in Appendix A.

telephone numbers, business faxes and business emails are *not* personal information under FIPPA.

How Personal Information May Be Collected, Used, Disclosed and Stored under FIPPA

- In the course of workplace activities or duties, public employees and service providers may **collect**[6] personal information for three main reasons:

    - under statutory authority;
    - for law enforcement purposes; or
    - for an operating program or activity of a public body.

  Teaching at a public educational institution is part of the operating program of that public educational institution.

- Personal information should be collected directly from the individual and the individual should be told why it is being collected.[7]

- Personal information collected must be accurate and individuals have the right to request correction of their information if it is inaccurate.

- Personal information collected must be protected with reasonable security arrangements.

  Examples of secure storage are locked cabinets, password-protected files and secure servers that prevent unauthorized access, collection, use, disclosure or disposal of personal information.

- **Storage of**[8] and **access to**[9] personal information must be in Canada, unless the individual has consented to it being accessed or stored elsewhere, or unless it is stored or accessed outside Canada for the purposes of disclosure specifically allowed under FIPPA.[10]

- **Disclosure** of personal information is permitted inside and outside Canada. Disclosure is permitted inside Canada with the individual's consent,[11] for a consistent purpose,[12] for health or safety reasons, in compelling circumstances, for law enforcement purposes and in other narrow and specific circumstances. "Consent"

[6] See the general definition for collection set out in the glossary in Appendix A.
[7] There are some exceptions to this requirement that account for law enforcement, health and safety situations. See section 27 of FIPPA.
[8] See the general definition of storage set out in the glossary in Appendix A.
[9] See the general definition of access set out in the glossary in Appendix A.
[10] An example of this might be for the purposes of law enforcement activities between international jurisdictions.
[11] See the general definition of consent set out in the glossary in Appendix A and discussed in Question 2. See also the definition of informed consent in Appendix A and discussed in Question 2.
[12] See the general definition of consistent purpose set out in the glossary in Appendix A.

means with the individual's approval and "consistent purpose" is a use of information that has a reasonable and direct connection to the original purpose of collection.

- Disclosure of personal information outside Canada is permissible for most of the same reasons as disclosure inside Canada, but does not include disclosure for a consistent purpose.

  Thus, disclosure of personal information outside Canada is significantly more restrictive and is often only achievable with the individual's consent.

- Unauthorized disclosure of personal information is prohibited and punishable. Public employees may be subject to a fine of up to $2,000 for privacy breaches and service providers up to $25,000.

To summarize, instructors in public institutions may collect, access, use, disclose (share) or store personal information in the course of their work activities, but must be careful to comply with the specific requirements, conditions and responsibilities of FIPPA as described above.

QUESTION 2
How do the issues of collection, use, disclosure and storage of personal information under FIPPA apply specifically to the use of social media in class?

When an instructor designs a class project or assignment using social media that requires the instructor to collect, use, disclose or store personal information, he or she is responsible under FIPPA for the appropriate protection of that personal information.

When an instructor designs a class project or assignment using social media that the instructor knows or expects may require his or her *students* to upload, share or store personal information, the instructor is arguably still responsible under FIPPA for the appropriate protection of that personal information. That is because the instructor has designed and set the course requirements and is the ultimate authority for student evaluation and grading in the course. To *what degree* the instructor carries FIPPA responsibility in this circumstance, however, is unclear. The privacy rules for social media are, as yet, untested at law in BC and instructors obviously cannot control the keystrokes of their students.

The best course of action, therefore, is for faculty to proceed from a position of caution. To accomplish this, instructors first should ensure that they are familiar with FIPPA's primary privacy requirements as set out above in Question 1 and, second, exercise due diligence in applying these requirements to course projects or assignments involving social media.

Faculty may also find it useful to focus their attention on three main privacy principles when designing course requirements: **notice**[13], **knowledge**[14] and **informed consent**.[15] Educating students about privacy and social media is another key element.

For example, where students may be required to upload, use or share personal information on social media as part of a class project or assignment, instructors should provide students with written notice of the purpose of the project or assignment, the technology to be used, what personal information may be required, why, the authority for requiring it and the potential uses of the information. Notice and knowledge should occur at the beginning of the course or project/assignment.

Instructors should also obtain their students' informed consent for any collection, use or disclosure of their personal information. Informed consent is typically requested and provided in written form and should be obtained *after* students have been made aware of the reasons, purposes, methods and implications for requiring their information.[16] Since obtaining consent is a key part of protecting privacy and exercising due diligence, instructors may want to establish a **privacy protocol**[17] for ensuring student notice, knowledge and consent whenever using social media as a teaching aid.

Finally, it is important for instructors to take the time to educate students about privacy when using social media in class. Since most social media web sites, services and applications permit quick, easy, wide and usually irretrievable dissemination of personal information, instructors serve their students well by providing them with key information about relevant privacy laws, practices and tools that students can use to better protect themselves online.

By using notice, knowledge and consent principles at each phase of the course development and delivery process, and by educating students in the appropriate use of personal information, instructors can readily prevent or mitigate many of the potential privacy concerns they may face when using social media in class.

---

[13] See the general definition for notice in the glossary in Appendix A.
[14] See the general definition for knowledge in the glossary in Appendix A.
[15] See the definition for informed consent set out in the glossary of Appendix A. See also the definitions set out in BC's *Freedom of Information and Protection of Privacy Regulation*, B.C. Reg. 322/93, O.C. 1281/93, September 22, 1993 (http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/11_323_93) and in Schedule 1, Principle 3, Section 4 of the federal government's *Personal Information Protection and Electronic Documents Act* (PIPEDA) (http://laws.justice.gc.ca/en/P-8.6/index.html).
[16] The notice and consent forms can be combined in one document. See the sample student consent agreement in Appendix B.
[17] See the general definition of privacy protocol set out in the glossary in Appendix A.

QUESTION 3
What specific steps can I take to ensure I am compliant with FIPPA when using social media for course assignments?

There are three main steps you can take to ensure compliance with FIPPA when using social media as a teaching aid. The purpose of these three steps is two-part: (i) to be aware of the technological capacities and privacy implications of the specific technologies you plan to use, and (ii) to engage appropriate privacy protections for using them.

Step 1 is to research the privacy strengths, weaknesses and policies of the social media you plan to use. Step 2 is to evaluate the identifiable privacy risks with respect to the privacy requirements of FIPPA. Step 3 is to develop a privacy protection plan and protocols for using the technology in class. These three steps are set out in detail below.

Step 1: Research the Technology

Ask: What are the privacy risks of using this technology?

- Who owns or maintains the technology? Is it a Canadian company? Foreign company? Open Source?
- Where is information uploaded to the technology stored? Where is the main server located?
- What information do I have to upload to use the technology? (i.e. just a name or other personal data?)
- Is there a user agreement? Does it say what information is collected and how it will be stored? Does it say who the uploaded information belongs to?
- Is there a privacy policy? Is it clear? Does it state how uploaded information will be used and if it will be shared with or accessible to others, such as fellow subscribers or other 3rd parties? (i.e. advertisers)
- Are there privacy controls or settings that users can activate? (i.e. ability to limit access to one's personal information or to opt-out of sharing it?)
- Does my IT department have privacy or security policies that may not allow the usage of this web technology? (There may already be established protocols.)
- Does my communications office or FOI/POP coordinator have institutional protocols in place for using web-based technologies? (Some technologies are regularly in the news as a result of ongoing privacy concerns or breaches.)
- Are there any published critiques of the technology on mainstream technology news or privacy web sites (i.e. CNET, Technology Review, PC World, EFF[18] and CIPPIC)[19] Are they positive? Negative?

[18] CNET is a free technology news and product review web site (http://www.cnet.com.) Other useful technology review sites are Technology Review published by MIT (http://www.technologyreview.com/) and PC World (http://www.pcworld.com).
[19] EFF is the Electronic Frontier Foundation, a privacy advocacy group based in the United States (http://www.eff.org). CIPPIC is the Canadian Internet Policy and Public Interest Centre (http://www.cippic.ca/en/).

- Are there other similar technologies I could use that are more privacy-sensitive and can achieve the same or similar results?

Step 2: Evaluate the Privacy Risks

Ask: Are the privacy risks of this technology reasonable in light of FIPPA requirements?

- Is the information uploaded by users stored inside or outside of Canada? If the server is inside Canada, the information might still be stored outside Canada on other servers either permanently or temporarily, which breaches FIPPA. This can be addressed in most cases by appropriate privacy-protection measures, which are discussed in more detail in Step 3 "Drafting a Privacy Protection Plan" and Question 4 "Privacy Tools" below.
- Does use of the technology require the uploading of extensive or particularly sensitive personal data, such as full name, physical address, age, gender, telephone number, etc.? If yes, this can often be addressed by the privacy-protection measures discussed below.
- Does the technology have a user agreement or privacy policy that adequately advises users how their information may be used or disclosed and are there privacy tools in the technology to mitigate exposure of personal information? Some technologies provide extensive privacy policies and options, such as opting-out of sharing information, but many do not. Some have long policies that purport to provide privacy protections and options but ultimately retain custody and control of all personal information, including photos.
- Can the technology be used in class in ways that avoid or significantly mitigate the identifiable privacy risks? For example, is uploading personal data necessary to the class assignment or can students use pseudonyms or avatars? Some technology experts advise never to upload genuine personal information, such as real names, birthdates, gender or photos.[20] Obtaining student consent or incorporating student user agreements are also options.[21]
- Are students willing and able to accept the responsibility of participating in the protection of their privacy? Some students may not want to use a new technology responsibly or use it all, which may put you, them and others at risk. If students cannot or will not comply with privacy-protection measures, are there other available options for them in completing the course assignment? Remember that requiring students to consent to use a technology that they do not want to use is essentially forcing consent, which is no consent at all.

[20] See: "Want to stay secure on Facebook, Twitter? Lie!", An Interview with Graham Cluley, Senior Technology Consultant, Sophos, by Dan Grabham, TechRadar, May 27, 2009. (http://www.techradar.com/news/internet/web/want-to-stay-secure-on-facebook-twitter-lie--602825)

[21] See Question 4 below for a full discussion of useful privacy tools.

Step 3: Draft a Privacy Protection Plan

Ask: Now that I know more about it, how will I use this technology and what privacy-protection measures can I employ to mitigate its privacy risks?

- Determine how much control you will exert over students' use of the technology, such as what the assignment will entail, what type of content will need to be uploaded and how the content will be used and shared. For example, will students be sharing information only with you, with each other or with a larger web community, such as on Facebook or Blogger?
- If you will have little or no control over what information will be uploaded or disclosed between students or other users, then consider drafting a student user agreement that clarifies the reason for using the technology in the class, the terms and conditions for uploading, using and disclosing personal information and the risks involved.[22] The student agreement is both an educational and risk-mitigation privacy tool.
- If uploading personal information is necessary to use the technology and complete the class assignment, then consider drafting a student consent agreement which clarifies this requirement, as well as what options are available for students who do not want to consent to the use of their personal information for the assignment.[23] Possible options may be pseudonyms, avatars or a choice of a different assignment.
- Prepare and present a brief seminar on privacy for students that sets out basic privacy principles, such as knowledge, notice and consent and the fundamental requirements of FIPPA. Identify best practices for students in protecting their personal information when using web-based technology, such as the risks of uploading or disclosing their or other people's personally-identifying information and the importance of and techniques for mitigating these risks.
- Prepare and distribute a privacy and technology tips sheet to students that gives them short, succinct advice to follow when using web-based technology.[24]
- Determine what options there may be for students who do not consent to the collection, use, disclosure or storage of their information on social media web sites. There should be an alternate choice for hesitant students unless privacy of their personal information can be guaranteed.
- Determine what steps or process you can or will resort to if there is a possible or actual privacy breach. You have a duty under FIPPA to both prevent and address breaches.
- Ensure you have notified your institution's FOI/POP Coordinator, technology department and communication office of your planned use of the chosen social media and that they are aware and supportive of the privacy plan and protocols

[22] See Question 4 for a full discussion of a student user or class agreement. See also Appendix C for a sample Student User Agreement Form.
[23] See Question 4 for a full discussion of a student consent agreement. See also Appendix B for a sample Student Consent Agreement Form.
[24] See Question 4 for a fuller discussion of the usefulness of a privacy and technology tips sheet. See Appendix D for a sample privacy and technology tips sheet.

you have developed to address privacy concerns. The head of your institution carries ultimate responsibility for breaches at the institution but employment and service agreements usually distribute the liability for acts of individual negligence or wrongdoing.

QUESTION 4
What specific tools or protocols can I use to ensure privacy-sensitivity in class and to help students to protect their own personal information?

There are four practical tools or protocols you can employ to encourage a privacy-sensitive environment[25] for students and to ensure due diligence in protecting personal information.

The first, and probably most important, privacy tool or protocol you can engage is to prepare or provide a brief privacy seminar for students that informs them about existing privacy legislation in BC and Canada and highlights the importance of fundamental privacy principles, such as knowledge, notice and informed consent. Most younger students have grown up in a culture of mass information-sharing and are not yet old enough—or simply have been fortunate enough—to never have suffered the serious negative consequences for sharing too much of their or other people's personal information.

Along with giving students important information about privacy law and practices, your presentation could invite student input and discussion about what privacy means to them and how sharing personal information can seriously impact people's lives. You may also like to share recent stories in the media that demonstrate the potential privacy risks and concerns associated with the information-sharing features and practices of popular social media giants. Providing students with such information about privacy is a significant way to educate and sensitize them to potential privacy issues, as well as to ensure you are exercising due diligence when employing social media tools for course projects or assignments.

A second useful privacy tool for instructors is the use of a student user agreement or class contract that sets out the name and purpose of the class project or assignment using social media, how the technology will be used and the class terms and conditions for the collection, use and disclosure of personal information in the course of the project. If presentation of the user agreement is preceded by a privacy seminar on FIPPA privacy principles and standards, then students will have a good understanding of how and why they should protect their personal information and that belonging to other individuals. The student user agreement is another important step in exercising due diligence when using social media in class.

A third effective privacy tool and protocol for instructors is the signing of a student consent agreement[26] when using social media that collects, uses or discloses personal

[25] See the general definition for privacy-sensitive environment in the glossary in Appendix A.

information. The consent agreement should state the name and purpose of the project, the name of the technology that will be used, the anticipated scope of its use in collecting, using, disclosing and storing personal information and the privacy implications and risks. Providing students with notice and knowledge of the nature and effect of using a particular technology for a class project or assignment and seeking their informed consent is not only an important step but a necessary one to ensure due diligence under FIPPA when using social media in class.

For students who do not provide their consent, instructors should offer an optional method for completing the class project or assignment without social media. As discussed in Step 2 of Question 3 above, forced consent is no consent at all within the meaning of standard privacy law and practice.

A fourth privacy tool for instructors is the distribution of a privacy and technology tips sheet.[27] A tips sheet provides quick and informative guidance on how to protect privacy online and is information to which students can independently refer when difficult questions or novel situations arise. Although the capabilities and risks of new technologies continually fluctuate and evolve, there are some standard practices students can follow to help them better protect their personal information in digital environments. The privacy and technology tips sheet also gives instructors additional assurance that they are exercising appropriate due diligence when using social media in class.

QUESTION 5
Where can I get more information or advice on particularly puzzling privacy questions or scenarios raised by using social media in class?

Your first and most immediate source for information about FIPPA compliance is your institution's FOI/POP Coordinator. Every public body in BC is tasked with the responsibility for its own compliance with FIPPA through the head of the institution. Typically however, the day-to-day responsibility for compliance and corporate education about FIPPA is delegated to a designated FOI/POP Coordinator or another senior corporate employee who manages FIPPA-related issues along with his or her primary duties. If you have questions or concerns about how to apply FIPPA in the course of your duties, one of your first steps should be to consult your FOI/POP Coordinator.

If your FOI/POP Coordinator is unable to assist you, he or she may contact the provincial government's Knowledge and Information Services Division (KIS)[28] of the Office of the Chief Information Officer (OCIO) whose mandate is cross-government privacy research, policy and legislation. Staff in this office are experts in privacy law and provide a helpline through which they can answer privacy questions from public body employees

---

[26] A template for a Student Consent Agreement Form is included in Appendix B of this guide.
[27] See Appendix D for a sample Privacy & Technology Tips Sheet.
[28] The web site for Knowledge and Information Services, Office of the CIO, Ministry of Citizens' Services is http://www.cio.gov.bc.ca/cio/kis/indexpage. Their helpline can be reached by calling Enquiry BC, listed in the blue pages of your local telephone book, and asking for the Privacy Helpline.

or service providers or can point you to further resources to get appropriate answers. There are also links on the KIS web site to an official copy of FIPPA and the FIPPA Policies and Procedures Manual[29] which has detailed explication of some of the prominent privacy requirements of the Act.

In addition to these direct sources, you can seek general input from the Office of the Information and Privacy Commissioner for British Columbia (OIPC)[30]. Although the Commissioner's Office is primarily tasked with mediating and adjudicating disputes between individuals and public bodies about FOI requests and privacy complaints, the Commissioner and staff also have a mandate to educate the public about FIPPA and will often provide public body employees or service providers with general feedback or recommendations. Some of the OIPC's intake and portfolio officers are particularly experienced in dealing with issues common to post-secondary institutions.

For more general information about privacy and technology issues or other emerging topics in privacy law in Canada or North America, you may find it useful to browse the web sites of either the Privacy Commissioner of Canada[31] or the Canadian Internet Policy and Public Interest Clinic (CIPPIC)[32]. The Privacy Commissioner of Canada's web site deals with federal public and private sector privacy law in Canada, as well as has numerous links and resources on other topical privacy issues of interest to North Americans. CIPPIC is very active in the privacy implications of emerging technologies.

There are also two prominent Canadian privacy and technology law experts in the Faculty of Law at the University of Ottawa: Dr. Michael Geist[33] and Dr. Ian Kerr[34] who provide a great deal of information on their web sites. Both Geist and Kerr hold research chairs in privacy and technology law in Canada and their blogs discuss some of the most topical privacy and internet technology issues in Canada and the world. Here in BC, Dr. Colin Bennett, Professor of Political Science at the University of Victoria, is a world-renowned privacy expert and author.[35]

Finally, the federal government's *Personal Information Protection and Electronic Documents Act* (PIPEDA)[36] and the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information [37] both set out and explain the primary privacy principles common to public and private sector privacy laws in Canada and other similar

---

[29] The BC government's FIPPA Policies and Procedures Manual is available on the OCIO's web site at: http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page

[30] The Office of the Information and Privacy Commissioner for BC's web site is: http://www.oipc.bc.ca.

[31] Office of the Privacy Commissioner of Canada (http://www.priv.gc.ca)

[32] Canadian Internet Policy and Public Interest Clinic (CIPPIC) (http://www.cippic.ca)

[33] Dr. Michael Geist, Professor of Law and Canada Research Chair in Internet and E-Commerce Law, University of Ottawa (http://www.michaelgeist.ca).

[34] Dr. Ian Kerr, Professor of Law and Canada Research Chair in Ethics Law and Technology, University of Ottawa (http://iankerr.ca/).

[35] Dr. Colin Bennett, Professor of Political Science, University of Victoria (http://www.colinbennett.ca/).

[36] A copy of PIPEDA is posted on Justice department's web site (http://laws.justice.gc.ca/en/P-8.6/index.html).

[37] CSA Model Code for the Protection of Personal Information, Canadian Standards Association (http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code/article/principles-in-summary)

national jurisdictions. The privacy principles in Schedule 1 of PIPEDA are drawn from, and are virtually identical to, the principles set out in the CSA Code. Their explanations of key privacy principles, such as the nature and meaning of informed consent, may be useful for instructors in understanding and explaining standard privacy principles and practices to students.

Conclusion

Ideally, the discussion, steps and tools presented in this guide answer the main questions arising for faculty members wanting to use social media as a teaching aid or tool in public post-secondary courses or programs. The guide summarizes the key privacy principles and requirements of BC's FIPPA legislation, as well as provides instructors with specific privacy-protective steps and tools they can use to ensure adherence to FIPPA and due diligence when using social media in class.

Carefully reviewing the privacy principles and requirements discussed in Questions 1 and 2, and proceeding through the privacy-protective steps set out in Question 3, will address many of the standard privacy questions or concerns raised by using social media in class. Engaging some or all of the privacy tools discussed in Question 4 and seeking assistance if required as addressed in Question 5 will provide additional assurance for instructors that they are creating privacy-sensitive teaching environments, maximizing the privacy awareness of their students and teaching students how to protect themselves, which is an eminently valuable collateral benefit.

Although the caution required when using social media may at times seem burdensome to instructors, it is nonetheless necessary to ensure compliance with FIPPA's privacy principles and to safeguard students. As privacy experts frequently profess, once privacy is lost it cannot be regained. Privacy-sensitivity to new technologies needs to occur at the *beginning* of the course development and delivery process, not in the middle when a privacy breach has occurred. If, after all cautions have been taken and a privacy breach still occurs and the individual harmed complains to the Information and Privacy Commissioner, then the instructor can show a history and record of due diligence in the planning and use of social media in class. This is an important illustration for the Commissioner of the instructor's commitment to privacy protection and compliance with FIPPA.

Aside from legal imperatives however, it is important to underscore that the most important aspect of privacy protection is simple education and awareness. Knowing why privacy is important and how to protect it is the first and best principle in preventing privacy breaches. The use of specific privacy tools and protocols to mitigate risk is the second major principle. If educators can integrate these two key principles into their regular course planning and delivery process where social media is being used, then they will ensure not only that appropriate privacy protection measures are in place but that students are educated to be privacy-sensitive themselves. This conscientious attention to the value and practice of privacy both upholds the privacy laws of BC and contributes to a positive and respectful learning environment.

Glossary of General Privacy Terms

Personal Information

The recorded information about an identifiable individual. Does not include business contact information in certain jurisdictions, such as British Columbia.

Record

Generally anything on which information is recorded or stored by graphic, electronic, mechanical or other means, such as books, documents, maps, drawings, photographs, letters, vouchers, papers, CDs, DVDs and other digital devices. Under BC's FIPPA, a record does not include a computer program or any other mechanism that produces records.

Collection of Personal Information

The amassing or uploading of recorded information about an identifiable individual.

Use of Personal Information

The reason for which recorded information about an identifiable individual is collected and how it will be engaged or applied.

Disclosure of Personal Information

The uploading, downloading or sharing by various means of recorded information about an identifiable individual.

Storage of Personal Information

The retention of personal information in the format of a paper or digital record in a specified location.

Access to Personal Information

The ability to retrieve and review personal information in paper or digital format.

Consistent Purpose

The use of personal information for a purpose that has reasonable and direct connection to the original purpose given for collection and that is necessary for performing the statutory duties or for operating a legally authorized program of the public body.

Appendix A: Glossary of Terms

Consent

The principle of seeking the permission and securing the agreement of an individual to the collection, access, use disclosure or storage of the individual's personal information. Consent, however, may be implied in some circumstances, such as where knowledge and notice are present. Consent may be given or obtained verbally or in written form, depending on the circumstances.

Informed Consent

The principle of seeking the individual's permission for, and securing his or her agreement to, the collection, access, use, disclosure or storage of the individual's personal information by providing the individual with sufficient notice and knowledge of the reason for, and the circumstances and implications surrounding, the proposed collection, use or disclosure. Informed consent is typically requested and provided in written form.

Notice

Verbal or written advisory provided to an individual stating that his or her personal information is required for a particular purpose and may or will be collected, accessed, used, disclosed or stored in a particular way, by a particular entity, in a particular place, at or for a particular time.

Knowledge

Verbal or written advisory provided to an individual that, in addition to basic notification, provides the individual with additional important and relevant details about the purpose, circumstances, consequences and implications surrounding the stated collection, access, use, disclosure or storage of the individual's personal information.

Privacy Protocol

Standards, processes or methodologies by which a person or organization establishes a regular or routine practice of protecting personal information, such as a methodology for obtaining informed consent.

Privacy-Sensitive Environment

A physical or digital interactive workplace, marketplace or social, health or educational community where individuals conduct themselves and their activities in a manner that respects the central privacy principles of notice, knowledge and consent when collecting, accessing, using, disclosing or storing the personal information of identifiable individuals.

Appendix B: Consent Agreement Template

Student Consent Agreement Form: Consent to the Collection, Use, Disclosure and Storage of Personal Information When Using Social Media in Class

This form is used to obtain your informed consent to the collection, use, disclosure and storage of your personal information when using 3rd party web-based technology (social media) in this course for a class project or assignment.

**Please carefully read, fill out and sign the form below. If you have any questions or concerns about the form or the protection of your privacy, please consult the instructor.*

****

Student Name: _____ **Date:** _____

Class: _____ **Instructor:** _____

Name and Description of the Project or Assignment, the Technology to be Used and the Reason for its Use in Class:

[Instructor: Insert the name of the class, project or assignment and identify the technology to be used, including how and why it will be used. Example: "As part of the research requirements for History 112, you will be asked to participate in, and help develop, a class "history wiki" by uploading your research findings on a weekly basis to the class wiki on Wikimaking.com.[38] The class wiki will be password-protected and restricted for use by class members only."]

Identifiable Privacy Risks:

[Instructor: Carefully review the user agreement and privacy policy of the technology with particular respect to how personal information may be collected, used, disclosed and stored by the host. Then insert a synopsis of the privacy concerns or risks as stated in the agreement or policy, how you perceive or project them to be and if there are privacy protection tools on the site that students can use.[39] Example: "Wikis created on the Wikimaking.com web site require users to register by uploading their username and valid email address. According to Wikimaking's user agreement and privacy policy, all personal information uploaded will be collected and stored by Wikimaking and may be shared with Wikimaking's clients. This means that students may receive 3rd party solicitation emails. Further, any information students upload to the wiki will be displayed with students' usernames and emails. To protect their privacy, students may

[38] Wikimaking.com is a fictitious social media web site created solely for the purpose of providing an example in this guide.

[39] The length and content of an identifiable privacy risks statement will vary greatly depending on the technology being used, the information in its user agreement and privacy policy and the instructor's purposes or goals in using the technology for the class project or assignment.

Appendix B: Consent Agreement Template

select opt-out options in the privacy controls section of the web site or use a non-identifying username and alternate (non-personal) email address when registering to use the site."]

Student Consent Statement:

I, _____, agree to the collection, use, disclosure and storage of my personal information inside or outside of Canada while using the technology described above for the purposes of engaging in this class. I am aware of and understand the identifiable privacy risks as described above and will endeavour to minimize exposure of my and other people's personal information by collecting, using and disclosing only that information that is necessary to complete the course in the manner prescribed by the instructor.

Where possible, and if approved by the instructor, I may use a pseudonym or remain anonymous online for the purposes of this class to minimize exposure of my or other people's personal information to 3rd parties that are not part of this class or project or who are otherwise not entitled to this information.

This consent is valid until _____ unless revoked by me in writing and delivered to the instructor.

Student Signature: _____ Date: _____

Appendix C: Student User Agreement Template

Student User Agreement Form: Terms & Conditions for Using Social Media in Class Projects or Assignments

This form is used to inform you of the terms, conditions and expectations for using 3rd party web technology (social media) in class for a class project or assignment.

**Please carefully read, fill out and sign the form below. Signing the form indicates your agreement to abide by the stated terms, conditions and expectations. If you have any questions or concerns about the form or your privacy, please consult the instructor.*

****

Student Name: _____ **Date:** _____

Class: _____ **Instructor:** _____

Name and Description of Class Project or Assignment:

[Instructor: Insert the name of the class project or assignment and provide a short description.]

Name of the Technology and Its Expected Use in Class:

[Instructor: Insert the name of the technology and describe how it will be used for the class project or assignment. Example: "As part of the research requirements for History 112, you will be asked to participate in, and help develop, a class "history wiki" by uploading your research findings on a weekly basis to the class wiki on Wikimaking.com. [40] The class wiki will be password-protected and restricted for use by class members only."]

Terms & Conditions for Uploading, Using and Disclosing (Sharing) Personal Information While Participating in an Online Class Assignment or Project:

I, _____, agree that I will adhere to the following terms and conditions when using the above-named technology for a class project or assignment. I realize that if I do not abide by these terms and conditions I may expose my or other people's personal information to unauthorized third parties, leading to an invasion of my or other people's privacy.

[Instructor: You may wish to insert a statement here regarding the consequences for disregarding the terms and conditions of the user agreement, such as loss of the privilege of participating in the online project or assignment, or some other result/effect.]

[40] Wikimaking.com is a fictitious social media web site created solely for the purpose of providing an example in this guide.

Appendix C: Student User Agreement Template

Specific Terms and Conditions

1. I will review the technology's functions, capabilities, user agreement and privacy policy before registering and engaging with the technology so that I am aware of the repercussions and conditions of using this technology.

2. If required to register for service on the technology by providing personal information, such as my family name, home address, telephone number, gender or birthdate/age, I will provide only the minimum personally-identifying information necessary to activate my account. I may provide my initials, a pseudonym or an alternate email address in place of personally-identifying information where the instructor advises it acceptable to do so.

3. I will not share my or the class password(s) with unauthorized individuals.

4. I will not allow other users to access or use my password or account.

5. I will familiarize myself with the technology's privacy controls and settings so that I may activate these controls and settings on my account where necessary or advisable to protect my privacy.

6. I will, at all times, use the technology in a privacy-sensitive manner, refraining from including my or any other identifiable individuals' personal information in posts, instant messages and email exchanges. Specifically,

    - I will not post or share my or anyone else's full name, home address, personal email address, telephone number, gender, birthdate/age or other potentially-identifying information.
    - I will not make statements or express opinions about my or any other identifiable individual's personal life or character.
    - I will not post or share information, images, audio or video belonging to or identifying other individuals without first seeking their permission and obtaining their consent.

6. I will immediately report any potential, foreseeable or actual privacy invasions to the instructor so that the problem, breach or error can be addressed and rectified.

7. I will follow the instructor's directions for the identified use and purpose of engaging this technology for the class project or assignment.

    [Instructor: Add here any other specific terms, conditions or expectations related to the use of the technology in class.]

Student Signature: _____ Date: _____

Privacy & Technology Tips Sheet: Protecting Your Personal Information Online

There are two main privacy concerns for individuals interacting online: **transactional privacy** and **content privacy**. Transactional privacy is privacy of the contact data that specifically identifies individual users or their computers (e.g. IP addresses) and what they access online, when, for how long and with whom. Content privacy is privacy of the actual words, views, opinions, images and relationships that individuals share, exchange or review online. The privacy and technology tips, below, are divided into these two categories for easy review.

Note: The tips are a compendium of standard, common-sense practice and educated advice provided to the public by recognized privacy and technology public advocacy groups, such as the Electronic Frontier Foundation (EFF), Center for Democracy and Technology (CDT), Electronic Privacy and Information Rights Center (EPIC), Privacy Rights Clearinghouse (PRC) and Canadian Internet Policy and Public Interest Center (CIPPIC). Please refer directly to their web sites (listed below) for additional detail and guidance. [41]

A. Protecting Transactional Privacy

Secure Your Computer

- Make sure your computer is secure. Install firewalls, anti-virus and anti-malware programs to prevent unauthorized access by online intruders who could install viruses, cookies and web bugs on your computer to track what you look at and who you communicate with, when and for how long. This information can be used to profile you.
- Turn on the cookie notice function in your web browser. Some web site cookies are used for data-mining or marketing purposes and can track what pages you load or what ads you click on and then share this information with their client web sites. This information can be used to profile you. (Advanced tip: Consider allowing "session cookies" only which allow you to access programs or services when you need them but deletes most cookies automatically when you log off.)
- Vary your IP address by turning off your modem when you finish with your computer for the day, and leave it off overnight. When you turn it on the next day, your IP address will change. Search providers and other services you interact with online can

[41] Electronic Frontier Foundation (http://www.eff.org.); Center for Democracy and Technology (http://www.cdt.org); Electronic Privacy and Information Rights Center (http://epic.org); Privacy Rights Clearinghouse (http://www.privacyrights.org); and Canadian Internet Policy and Public Interest Center (http://www.cippic.ca).

see your IP address (unique to your computer) and link it with all your web searches. This can be used to profile you.

Use Search Engines and Web Browsers Wisely

- Turn on your web browser's "clear history" and "clear cookie" functions so the record of sites you visited or cookies you accepted is automatically deleted once you log off. If you are using a public computer then activate the erase history function on the browser as you log off.
- Configure your web browser to protect your personal information. In the "set-up", "preferences" and "options" menus where your personal information is requested, use a pseudonym instead of your real name, an alternate email address that you use for public email rather than your personal one (or use the legitimate but non-personal someuser@example.com address if you won't need to check reply email) and don't provide any other personal information if you do not have to.
- Check your system-wide default mechanisms that manage web browsers and other internet tools and make sure you anonymize them too.
- Don't use your Internet Service Provider's (ISP) search engine for searches. Your ISP already knows who you are from your registration information and will be able to link your identity to all your searches. This can be used to profile you.
- Don't login to (customize) your search engine. Although logging in provides you with a personalized page, images and tools to use, it also links all your searches with your identity. This can be used to profile you.
- Don't download search engine toolbars. They may permit the collection of information about your web-surfing habits, which can be used to profile you.
- Don't enter sensitive personal information, such as telephone or social insurance numbers or other identifying financial or health information as search terms. They may be linked by service providers with other aspects of your identity or captured by hackers or identity thieves.
- Consider exploring and using search engines that claim not to collect any personal information at all, such as Ixquick (http://ixquick.com) and DuckDuckGo (https://duckduckgo.com).

Email and Instant Messaging

- Avoid using the same web service for both your email and your search engine (e.g. Google and Gmail). If you do, your email will be linked to your searches, search terms and search history. This information can be used to profile you.
- Delete email regularly—every week or month, for example. Keeping it indefinitely allows your email provider to profile you for targeted advertising. Also, if a hacker or identity thief strike, they will be rewarded with a huge cache of your personal information.
- Don't reply to spammers—even to say "remove me from your list." That only confirms for them that your email is "live" and you will probably receive more. Also the "unsubscribe" options they provide can be bogus so ignore them. Activating an "unsubscribe" option may simply land you on dozens more spam lists.

- Defeat web bugs (graphic emails that enable the sender or a 3rd party to monitor who is reading its message or linking to its web page) by downloading your emails then opening and reading them offline.
- All email and instant messaging (IM) programs have archiving capabilities. Pressing the delete button may delete the message from your view and prevent your retrieval of it, but the messages are still retrievable by the service provider. In fact, some IM programs automatically save your chats unless you proactively select otherwise. Look for features on your IM service that allow you to prevent recording or archiving of your conversations. Remember, though, that email in particular is virtually always saved on back-up tapes.

Select Good Passwords and Use Them Effectively

- Develop strong (complex) and varied (multiple) passwords for your programs and functions and never write them down.
- Use nonsensical (except to you, of course) combinations of letters, numbers and symbols for your passwords.
- When you type in passwords, consider typing the characters out of order so that keystroke spyware cannot record them correctly. For example, instead of typing "daisyface24", try typing only "dais4" at first, then go back to fill in the missing piece of the phrase in the middle, which is "yface2". This technique will allow you to login to webmail and other accounts from public computers more safely.

B. Protecting Content Privacy

Choose Internet Applications, Services and Web Sites Carefully

- Investigate new applications, services and web sites before you use them. Choose ones with good reputations and that have privacy policies.
- Understand the basic functionality of each application, service or web site before you upload any personal information to it and read their service agreements and privacy policies carefully. Although they may be long or complex, reading policies and agreements is essential to gleaning an appreciation for the privacy risks involved.
- Remember that if you are uploading or creating words or images on 3rd party web sites, such as Picasa, Facebook and YouTube, the information is stored on their servers, so if the web site, service or application is sold or goes bankrupt, the privacy and security of your information may change regardless of what the original service agreement or privacy policy says.
- Consider that the best protection for your personal information is to not upload it in the first place or to anonymize it or to use pseudonyms, aliases and alternate/protected identities wherever possible. Be sure to read the user agreements, though; some hosts deny access to their services for users that provide false information, so be aware of the risks before taking them.

Appendix D: Sample Privacy and Technology Tips Sheet

Read Privacy Policies and User Agreements

- Yes, they are often long and boring but they are important. Pay particular attention to the part of the user agreement or privacy policy that explains how the host will collect, use, share and store your personal information and who it says owns the information (including photographs and other images) uploaded or created while using the application, service or web site. It is typical for hosts to claim some form of access or control over your words and images, such as the right to share it with 3rd party clients, so be prudent and selective about what you think is reasonable or fair.
- Check to see if the user agreement requires you to register to use the service and if you have to supply your real name, email address or other personal information. Some agreements say that you will forfeit service or face some other penalty if you provide incorrect or misleading personal information. It is up to you to decide what information you will provide and what risks or consequences you will accept for protecting personal information by using pseudonyms, aliases or alternate email addresses.
- Look for a statement in the user agreement about cancellation of your account. Does the host allow it or are you only able to "deactivate" your account. Does the agreement clarify what happens to your information if you cancel your account?
- Be suspicious of privacy policies that are hard to find on the host's web site or that are vaguely or confusingly written. Privacy policies do not have to be long to be good, but they should be clear and accessible. Ideally there should also be a number or contact person listed who can explain or answer questions about the privacy policy.
- Look for a statement in the privacy policy about how or where to complain if you are unhappy about the collection, use, disclosure or storage of your information. There should be a process for complaining and a person who has authority for handling complaints about policies and breaches.
- Check to see if the host participates in a "privacy seal" program. Sites and services that do participate in privacy programs show some level of commitment and concern for users' privacy, and the program may provide an alternative source of resolution for complaints. Some examples of reputable privacy seal programs are: Verisign (http://verisign.com) and Truste (http://www.truste.com). Privacy seals, however, are not guarantees of privacy protection.
- Look to see how the privacy policy or host states it will address or manage changes to its privacy policy. Will it notify you by email, announce changes prominently on its web site or just simply modify the policy? The way a host makes changes to its policy reflects its respect for the privacy principles of notice, knowledge and consent.

Blog with Care

- Choose a blog service carefully. Some automatically show your personal information by your posts. Only use blog sites that allow you some control over how much information you make public.
- If you are writing a blog, consider who your audience is or who you want it to be. If it is only for family, friends or other small group, consider requiring a password for access to the blog. If for a larger audience, remember that what you say and how you say it may be archived and accessible to all for many years to come.

Appendix D: Sample Privacy and Technology Tips Sheet

- To ensure your blog remains anonymous, register your domain name anonymously, since anyone can look up a blog in WHOIS to discover who owns the domain name.
- If you are commenting on a blog, think carefully about how much personal information and opinion you want to reveal or comment anonymously by using a pseudonym, alias and alternate/non-identifying email address.

Use Email and Instant Messaging Cautiously

- Virtually all email and instant messaging systems have archive functions and some even have recording functions, so anything and everything is conceivably retrievable even if you think it is transitory or has been "deleted". (See discussion of email and IM above under transactional privacy.) Further, your correspondent may decide to copy or record and redistribute your conversation. So even if the privacy and security of the technology and host you are using are reputable and reliable, your communications may still be recorded, copied, printed off or posted somewhere else without your knowledge or consent. Be cautious!
- Do not send or respond to personal email on mailing lists. With the click of a button or a processing error your messages could inadvertently go to everyone or the wrong people on the list.
- Don't say or share things in an email or instant message that you would not be comfortable seeing printed on the front page of your local newspaper. Sending or posting your most personal thoughts or images on the internet is tantamount to publishing them—unless you use an encryption program. Email encryption allows the sender of an email to scramble or encode messages so that only the designated receiver can unscramble them with the help of a special key (code).

Social Network Safely

- Be your own best protection! Don't post or share your personal information online, especially on pages where "new friends" or strangers can view it. Social networks are rife with hackers and identity thieves looking for victims. Rely on yourself as a first-line privacy defence.
- Make sure you search for and activate the privacy options and tools available on social networking sites, such as features allowing only known, trusted or approved family and friends to access your profile, personal pages or updates. Many social networks do not provide significant or reliable privacy options, but, if they do, activate them! Remember, though, that even with privacy protections, breaches can and have occurred, so don't rely solely on the technology to protect your content.
- Look in particular for privacy-based "opt-out" options on the network so you can limit viewers' access to your user/client information. Better yet, use pseudonyms, aliases and alternate email addresses wherever possible or reasonable. Any personal information viewers can see on your user profile may be used to find or profile you.
- Finally, be cautious and sensitive to the ramifications of what you post about yourself or anyone else online. Little words can lead to big harm and ruin friendships, careers and even lives, so be vigilant in protecting your own privacy and respectful of everyone else's.

Contact Information

- For more information about the contents of this guide or to request assistance in developing additional privacy materials or presentations for your public or private sector group or institution, please contact:

Pamela Portal, B.A., LL.B.
Privacy Research, Policy and Communications Consultant
Tel: 250.418.1626
privacyguide@shaw.ca

- For more information about BCcampus and the Shareable Online Resources Repository (SOL*R), please contact:

Paul Stacey
Director, Communications, Stakeholder and Academic Relations
BCcampus
paul.stacey@bccampus.ca