THE UNIVERSITY OF BRITISH COLUMBIA

Office of the University Counsel
6328 Memorial Road
Vancouver, BC V6T 1Z2
Fax: 604-822-8731

From: Office of the University Counsel

Date: September 2010

RE: Email and Privacy Legislation

Below are responses to the questions that have been asked with respect to the *Freedom of Information and Protection of Privacy Act* ("FIPPA") and email. Further, also enclosed at the end of this memo the relevant sections of FIPPA that were noted.

Most important:

1) Is email subject to the Freedom of Information and Protection of Privacy Act (FIPPA)?

   Yes, email is subject to FIPPA. Any record in the custody or under the control of UBC is subject to the legislation with a few exceptions that are outlined in section 3 of FIPPA. For example, exams and teaching materials are not subject to FIPPA.

   FIPPA defines a record to include books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

2) If so, what is considered to be 'personal' or 'private' information? Are photos, video, etc. (containing students, faculty or staff) considered 'private' information?

   FIPPA defines personal information as recorded information about an identifiable individual other than contact information. Contact information means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

   Photos and videos of identifiable individuals are considered personal information.

3) Does the University of British Columbia have any legal obligation to ensure that email relating to University business remains within Canada?

Yes. University business should not be conducted on systems outside of Canada. All Personal Information in the custody or control of the University must be stored only in Canada unless appropriate written consent has been obtained from the individual whom the Personal Information or if permitted by law. (Section 30.1)

Care needs to be taken when considering using services provided by third parties since a majority of third party service providers (Hotmail, Gmail, etc.) store data outside of Canada. In addition, linking UBC email accounts to outside service provider accounts is also not appropriate.

4) Can a UBC student, faculty or staff member consent to allow personal information to be hosted outside of Canada? Note that personal information belonging to others may be forwarded to this external email account without that person's consent.

A person can consent to his/her own information being stored and/or hosted outside of Canada. Please note that the consent is only for a specific person's personal information. A person cannot consent to forwarding another individual's personal information.

5) How long must email containing personal information be retained and is it the responsibility of the individual or email service provider to retain copies to these messages?

The only retention requirement under FIPPA is that personal information must be retained for a minimum of one year from the date it was used to make a decision that affected an individual so the individual has the opportunity to access the information. (Section 31)

What should the retention and destruction schedule be for UBC email?

I recommend that you consult with Alan Doyle, UBC Records Manager, in UBC Archives. He works with units to develop appropriate retention schedules that consider all factors including relevant legislation.

6) What email practices should UBC instructors follow when communicating with UBC students and colleagues? E.g. Require students to use UBC address?

Email is not confidential and secure. Care must be taken when using email to communicate with students. Very confidential or sensitive personal information should not be communicated via email. A more secure method should be chosen. Further, since email is considered a record under FIPPA,

it is subject to the legislation. Individuals should be aware that there is a possibility that email may be disclosed in response to a request under FIPPA therefore it is important to use appropriate style & language when communicating via email.

7) What are the consequences of not abiding by FIPPA in relation to email usage?

UBC cannot be in breach of FIPPA because then we may be brought before the Information and Privacy Commissioner at the Office of the Information and Privacy Commissioner in Victoria for violating the requirements of FIPPA.

Process Questions:

1) Should students be allowed to see email addresses belonging to other students in their classes or at UBC?

It should be a student's choice on whether they want his/her email address visible.

2) Should students be allowed to see free/busy time in calendars belonging to others students at UBC?

As above, it should be a student's choice on whether or not he/she wants to make his/her calendar visible to other UBC students.

Relevant sections of FIPPA

Scope of this Act

3 (1) This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following:

(a) a record in a court file, a record of a judge of the Court of Appeal, Supreme Court or Provincial Court, a record of a master of the Supreme Court, a record of a justice of the peace, a judicial administration record or a record relating to support services provided to the judges of those courts;

(b) a personal note, communication or draft decision of a person who is acting in a judicial or quasi judicial capacity;

(c) subject to subsection (3), a record that is created by or for, or is in the custody or control of, an officer of the Legislature and that relates to the exercise of that officer's functions under an Act;

(c.1) [Repealed 2002-50-19.]

(d) a record of a question that is to be used on an examination or test;

(e) a record containing teaching materials or research information of employees of a post-secondary educational body;

(f) material placed in the archives of the government of British Columbia by or for a person or agency other than a public body;

(g) material placed in the archives of a public body by or for a person or agency other than a public body;

(h) a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed;

(i) a record of an elected official of a local public body that is not in the custody or control of the local public body.

...

Protection of personal information

30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Storage and access must be in Canada

30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

(a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;

(b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;

(c) if it was disclosed under section 33.1 (1) (i.1).

Retention of personal information

31 If an individual's personal information

(a) is in the custody or under the control of a public body, and

(b) is used by or on behalf of the public body to make a decision that directly affects the individual, the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information.