a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Office of the University Counsel
6328 Memorial Road
Vancouver, BC Canada V6T 1Z2

Phone 604 822 2451
Fax 604 822 8731
access.and.privacy@ubc.ca

Privacy Fact Sheet

Privacy of Email Systems

Introduction

1. The purpose of this Privacy Fact Sheet is to answer some common questions about the application of the *Freedom of Information and Protection of Privacy Act* (FIPPA) to UBC work email systems, such as FASmail. This Fact Sheet does not apply to email systems intended for personal use, such as the Student and Alumni Email System.

2. This Fact Sheet is intended to assist UBC staff and faculty members to understand their obligations under FIPPA. It is not a substitute for legal advice. If you have questions about FIPPA, contact the Office of the University Counsel.

Are Emails Subject to FIPPA?

3. FIPPA restricts how UBC collects, uses and discloses "personal information", which is defined as recorded information about an identifiable individual other than business contact information. All information about students is personal information, but the names and work contact information of employees are not. For more information, see the Privacy Fact Sheet What is Personal Information?

4. When UBC work email systems are used to transmit personal information, this personal information is subject to the protection of privacy requirements of FIPPA.

5. In addition, FIPPA allows members of the public to request access to "records" held by UBC, subject to limited exceptions. Emails are considered to be records. Therefore, individuals should be aware that there is a possibility that work-related emails may be disclosed in response to an access request under FIPPA. For more information about access requests, see UBC's Access and Privacy Webpage.

Are Email Addresses Confidential?

6. Work email addresses (e.g. john.smith@ubc.ca) are not confidential (because they are business contact information, which is public information). Many work email addresses are published on the directory on the UBC website.

7. The UBC email addresses of students and alumni (e.g. john.smith@student.ubc.ca and john.smith@alum.ubc.ca) are considered to be personal information, published on internal directories and may be used internally for UBC purposes.

8. Other personal email addresses are considered to be personal information and must not be shared with others without the recipient's written consent.

9. When sending emails to multiple personal email addresses, you must not place student or personal email addresses in the "To" field because you will expose the email addresses to the other recipients. To hide the email addresses, you must place them in the "Bcc" (blind carbon copy) field.

Is Calendar Information Confidential?

10. For work accounts, free/busy information is not considered confidential, provided that no information about the appointment is visible. However, you must not disclose the contents of the calendar entries unless you are certain that they do not contain confidential or personal information.

Can I Include Personal Information in my Emails?

11. Emails sent between UBC work email accounts are relatively secure. It is acceptable to include small amounts of personal information (and other information of a confidential or sensitive nature) in the body of these emails. However, when you are sending large volumes of personal information, or when the information is highly confidential (e.g. personal health information), you should place this information in an encrypted attachment to the email. Encryption is a process of "scrambling" information to make it unreadable to anyone who does not possess a key. Instructions for encrypting Word and Excel attachments are available on the Information Security website.

12. Emails sent from UBC work email accounts to external email accounts are not a confidential and secure method of communication. Therefore, you must exercise extreme caution when emailing personal information (and other information of a confidential or sensitive nature) outside UBC.

> An administrator sends an email to a faculty member alerting her that a student will be absent from classes for the next month. It is acceptable to include the name and student ID of the student in the body of the email. If it is necessary to share details of the student's medical condition, this information should be placed in a separate encrypted attachment.

Can UBC's Email System be Hosted Outside Canada?

13. FIPPA prohibits UBC from storing sensitive personal information outside Canada unless a Privacy Impact Assessment has been conducted that considers the risks of the foreign storage. UBC's work email system is hosted in Canada.

14. The majority of third party email providers (Hotmail, Gmail, etc.) cannot be used for UBC business purposes because they store data outside Canada and have not been approved through the Privacy Impact Assessment process.

Can I Check My Emails When I am Travelling Outside Canada?

15. Yes. Temporary access from outside Canada is allowed.

How do I Respond to Emails from Accounts Hosted Outside Canada?

16. Many students use Hotmail or Gmail accounts, which are hosted outside Canada. If a student or another party initiates contact with you using such an account, it is acceptable for you to respond to their email and to discuss the individual's personal situation if the individual requests you to do so. However, you cannot disclose information about anybody else.

Can I Use my UBC Email Account for Personal Purposes?

17. While work email accounts are intended for official use, UBC policy authorizes the incidental personal use of these accounts, provided such use does not interfere with the user's job performance and is not otherwise an inappropriate use under relevant policy or legislation.[1] An example of an "incidental personal use" of your UBC email account would be sending a short message to a friend inviting him to lunch. You should not use your UBC email account for long or sensitive personal communications.

18. If you use your UBC email account for personal uses, keep in mind that your communications may not remain private. While the University does not, as a routine matter, inspect personal emails stored on UBC email accounts, it may need to access these emails under certain circumstances, e.g. responding to lawful subpoenas or court orders; investigating misconduct and determining compliance with University policies; and searching for electronic messages, data, files, or other records that are required for University business continuity purposes.

Can I Auto-Forward my UBC Email Account to a Non-UBC Account?

19. Automatically forwarding or redirecting UBC email accounts to a non-business email account (e.g. a personal Gmail, Hotmail or Yahoo account) is not permitted under UBC's Information Security Standards[2]. Auto-forwarding to non-UBC corporate/business email accounts is only acceptable for UBC faculty and staff members who have employment or appointments at other organizations and are unable to manage multiple work email accounts. Under these circumstances, auto-forwarding is acceptable if:

    a. the other organization is a public body located in British Columbia and is subject to the *Freedom of Information and Protection of Privacy Act*, including the associated data residency and security requirements; and

    b. the faculty or staff member ensures that copies of emails are retained on or copied to UBC Systems in accordance with UBC's Records Management Policy.

20. Auto-forwarding to non-UBC business email accounts outside of the circumstances set out in paragraph 19 is prohibited unless the user has submitted a UBC Email Auto-forwarding Agreement and it has been approved by the Administrative Head of Unit and Chief Information Security Officer.

21. For example, UBC faculty members who work at Vancouver General Hospital generally use email accounts supplied by Vancouver Coastal Health (VCH). It is acceptable for these individuals to auto-forward their UBC email accounts to their VCH accounts. Most emails do not have to be retained because they are transitory in nature, or are copies of records that exist elsewhere. However, any emails which are considered to have evidential value must be retained so that they are secure and accessible to other UBC employees in the event they are needed. This may require printing them to paper, retaining a copy in a UBC email account, or capturing them in an electronic record keeping system.

22. Except as provided above, auto-forwarding is prohibited, for the following reasons:

    a. Privacy: Many UBC emails contain personal information, and FIPPA requires UBC to ensure that this information is adequately protected from unauthorized access.
    b. Security: Some UBC emails contain confidential or sensitive information. This information may not be adequately protected if it is stored on an external account.

[1] *Policy SC14*
[2] *Information Security Standard U3, section 4*

c. Records management: UBC's Records Management Policy requires staff and faculty members to manage and preserve records of value, which includes email messages. Emails that are stored on external email accounts may not be preserved as required under that policy.

23. UBC's Information Security Office can provide more advice about whether an institution's email system complies with the above requirements.

Can I Link my UBC Email Account to a Non-UBC Account?

24. Linking is a process where you give an external service provider your UBC CWL username and password so that it can download new emails on your behalf. You are not permitted, under any circumstances, to link your UBC email account to an outside service provider account. Sharing your CWL credentials with a third party is a serious violation of UBC information security policy.

Can I Access my UBC Email Account Using a Mobile Device?

25. You may only use a mobile device, such as a smartphone, to access your UBC email account if proper security controls are in place. If emails or other sensitive documents are stored on your mobile device, they should be encrypted. For more information about the security of mobile devices, see the Information Security website.

How Long Do I Have to Retain Emails?

26. Each email is a separate record that must be retained for the length of time prescribed in the applicable Records Retention Schedule issued by the Records Management Office under UBC's Records Management Policy.

27. In FASmail (UBC's primary work email systems) the contents of the deleted items, junk email and RSS feed mailbox are automatically deleted after 90 days. Inactive FASmail accounts are deleted after one year. For more information about these special email retention periods, contact the Records Manager in the Records Management Office.

What are the Consequences of Breaching FIPPA?

28. A breach of FIPPA may constitute an offence and may be subject to investigation and sanctions by the Information and Privacy Commissioner. In addition, it may result in disciplinary action by UBC.