THE UNIVERSITY OF BRITISH COLUMBIA

UBC Health

Guidelines for UBC Health Email Communications

To provide guidelines to UBC Health Programs regarding email communications

APPROVAL DATE: JUNE 2017
LAST REVISION: APRIL 13, 2017
DOCUMENT NUMBER: PEC – 1 DRAFT V.1

THE UNIVERSITY OF BRITISH COLUMBIA

UBC Health

CONTENTS

THE UNIVERSITY OF BRITISH COLUMBIA

UBC Health

TITLE

Alumni Email Address Policy

APPLICATION

These guidelines apply to staff, faculty and pre-licensure students in UBC Health Programs

INTRODUCTION

Prepared for review by the UBC Health Practice Education & Curriculum Committees
The document is based on Office of the University Counsel's recommendations regarding the Privacy of Email Systems, in particular, the Privacy Fact Sheet. These guidelines are intended to complement the BC Freedom of Information and Protection of Privacy Act (the "FIPPA"); the UBC Policy #104 Acceptable Use and Security of UBC Electronic Information and Systems; and Professional Standard for Learner and Faculty Members in the Faculties of Medicine and Dentistry at the University of British Columbia (2013).

Electronic documents pertaining to University business have the same legal status as paper documents, and are subject to all regulations and policies governing University data and information (including records management). Email used for conducting University business from on or off-campus, even if using a personal email account and/or a personally owned computer, is considered University property and subject to the Freedom of Information and Protection of Privacy Act (FIPPA).

GUIDELINES

1. General:

1.1 UBC Staff/Faculty should use their UBC FASmail account when communicating with students and as a means of communication for any other University business.

1.2 UBC Staff/Faculty/Students should *encrypt* emails when sending large volumes of personal information or when sending highly confidential information (e.g., student assessments or performance/behavioural issues, personal health information).

1.3 UBC Staff/Faculty must NOT auto forward faculty@mail.ubc.ca / faculty@ubc.ca emails to Gmail or Hotmail or any other email accounts hosted outside of Canada.

1.4 Students must activate and use their UBC Alumni hosted mailbox for educational purposes for the duration of their health program. Each student is expected to check her or his official email address frequently in order to stay current with program and University communications.

1.5 Students must use their UBC Alumni or health authority assigned email (where appropriate) if required to contact/correspond with preceptors or colleagues via email. While on placement/clerkship, please refer to the health authority guidelines for emails that may contain personal information related to patient care (e.g. http://vchnews.ca/wp-content/uploads/2017/09/Emailing-Guidelines.pdf).

1.6 Students must use their UBC Alumni email to create an account on the LearningHub portal (http://learninghub.phsa.ca/Learner/Home).

2. Exceptions:

2.1 Established practice education employer’s guidelines may differ and take precedence from what is outlined above (e.g., Vancouver Coastal Health [VCH] will give instructors/faculty a VCH email address using the format E12345 and students S12345.)

DISCUSSION

Faculty, staff and students are expected to familiarize themselves with applicable legislation, rules, regulations and guidelines. Failure to do so will not be an acceptable excuse for inappropriate behaviour during curricular or practice education experiences.

FIPPA requirements:

When UBC work email systems are used to transmit personal information, this personal information is subject to the protection of privacy requirements of the FIPPA (Freedom of Information and Protection of Privacy Act) legislation. 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 (e.g. student/employee number). 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.

Emails sent from UBC email accounts to external email accounts (such as Yahoo, Hotmail, Gmail, etc.) 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. If you are using the UBC email forwarding service, your email is only as secure as your destination email account.

It is recommended that Faculty/Staff use UBC's email system when communicating with students (e.g., faculty@mail.ubc.ca / faculty@ubc.ca to student@alumni.ubc.ca) because UBC's email system is secure and hosted on campus to ensure compliance with privacy and security requirements.

Important note: For security and privacy reasons, automatic email forwarding from the UBC Faculty & Staff Email (FASmail) service to *private* email accounts, such as Gmail or Hotmail accounts, is prohibited. However, forwarding FASmail accounts to email accounts at other public sector institutions is acceptable under limited circumstances. Before you proceed with these instructions, please review the Privacy Fact Sheet from the Office of the University Counsel on the Privacy of Email Systems, in particular, paragraphs 18 to 21 ("Can I Auto-Forward my UBC Email Account to a Non-UBC Account?")

HSPnet placement requirements:

Student@alumni.ubc.ca email addresses are required for registration and student access within HSPnet and Health Authority intranets. Student email address (student@alumni.ubc.ca) may be released directly by health programs to support administration of computer access at the placement site.

Records Management:

Emails that support the decision-making process at the University are considered to be University records and need to be managed/retained centrally (e.g., an email that documents a decision about an approval of an expenditure; outlines a project plan; or stipulates an accommodation for a specific student). When conducting University business via email, employees must use University provided account. When storing emails, be sure that the central storage location has the appropriate security.

Individuals should also be aware that there is a possibility that work-related emails may be disclosed in response to an access request under the FIPPA.

Students get to keep their @alumni.ubc.ca email address and UBC-hosted mailbox (if selected) even after they graduate or leave UBC.

Email issues with other email services and FASmail:

Yahoo, Comcast and AOL have recently updated their *DMARC* policies to proactively protect their users from spam that spoofs their email addresses on other mail servers. All *DMARC* compliant mail receivers (such as Yahoo, Hotmail, Gmail, etc.) reject emails sent as @yahoo.com, @comcast.net or @aol.com if they aren’t sent through the appropriate mail servers.

Student users who receive emails from Yahoo, Comcast and AOL addresses and are redirecting emails on FASmail via a redirect rule or an external contact to one of these *DMARC* compliant mail receivers may experience one of the following behaviours:

1. Emails are placed in Spam / Junk folders, sometimes with a warning stating their systems could not verify that this message was sent by the sender’s domain

2. Emails are dropped completely by the mail receiver (i.e., Gmail) with no *bounce-back* message sent to the sender
3. Emails are rejected by the mail receiver (i.e., Hotmail) with a *bounce-back* message.

For student ALUMNI email users who have a rule set up to redirect their emails, we recommend that they modify that rule to also keep a copy of messages in their FASmail Inbox. This will allow them to review any emails that were not redirected due to this *DMARC* policy.

Students may check their alumni email here: UBC Alumni Email Address

DEFINITIONS

The following definitions apply to these guidelines:

Bounce-back Message – an automated email response from a mail system informing the sender of a previous message that the message had not been delivered (or some other delivery problem occurred).

DMARC – “Domain-based Message Authentication, Reporting & Conformance”; this is an email authentication, policy, and reporting protocol. It adds linkage to the author domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, in order to improve and monitor domain protection from fraudulent email (https://dmarc.org/)

Encryption – this is the process of making information unreadable, in order to protect it from unauthorized access. Encryption creates a secret key or password that is necessary to unencrypt information and make it readable.

Private Emails – inclusive of Gmail and Hotmail accounts; these are email addresses, which should not be used for UBC-related correspondence.

UBC Health Programs – inclusive of Faculty of Dentistry, Faculty of Medicine, School of Nursing, Faculty of Pharmaceutical Sciences, School of Social Work, School of Audiology & Speech Sciences, Department of Occupational Science and Occupational Therapy; Physical Therapy, Genetic Counseling and Dietetics.

KEY RELEVANT DOCUMENTS

Include the following:

Personal Information Protection Act

Freedom of Information and Protection of Privacy Act (FIPPA)

Information Security Standard #05 Encryption Requirements

DOCUMENT MANAGEMENT AND CONTROL

Owner: UBC Health

Content manager: UBC Health Practice Education Committee

Date approved: Consideration of draft V.1: March 2017

Review date: This document shall be reviewed every (2) years and after approval, and thereafter as deemed necessary by PEC