Name:	**Email Policy**
Policy Number:	2-2006
Approving Authority:	President
Approved:	January 6, 2022
Responsible Office:	Enterprise Information Technology
Responsibility:	Chief Information Officer
Revision Date(s):	Not applicable
Supersedes:	2-2001 University Email Procedures and Guidelines
Next Required Review:	January 2025

1. Preamble

1.1 The University's email services support the educational and administrative activities of the University and serve as the means of official communication by and between Users and the University. However, use of an email system at the University requires adequate security measures to protect University data, and standards of use to comply with legal obligations with respect to freedom of information, privacy, and recordkeeping.

2. Purpose

2.1 This Policy requires the use of official University email accounts for the conduct of University business and describes acceptable use of University email facilities. The Policy also defines the responsibilities of all users of university email facilities, and the terms and conditions of use of official University email accounts. The purpose of the Policy is to ensure that this critical service remains available and reliable and is used for purposes appropriate to the business of the University.

3. Jurisdiction/Scope

3.1 This Policy applies to all members of the University community who are entitled to email services and to whom the University has issued an Official University email account, as detailed in this Policy.

3.2 The Chief Information Officer is responsible for the interpretation of this Policy.

4. Definitions

4.1 For the purposes of this Policy:

a. **"EIT"** mean the Enterprise Information Technology department of the University.

b. **"Email"** means written messages distributed by electronic means from one computer user to one or more recipients via a computer network.

c. **"FOIPOP Act"** means the Freedom of Information and Protection of Privacy Act (Nova Scotia), as amended from time to time.

d. **"Official University email account"** means an account with an email address ending with "smu.ca" issued to an authorized User by EIT. An official University email account is provided to members of the University community and may be granted to other individuals and entities who have been given email privileges at the University. It is automatically created for admitted and enrolled University students and actively employed faculty and staff.

e. **"University email facilities"** includes all University EIT assets, including facilities, hardware, software, and services required to accomplish the processing, storage, transmission, and communication of email, whether individually controlled or shared, stand-alone, or networked; University email facilities include official University email accounts.

f. **"User"** is anyone who is assigned an official University email account and uses or attempts to use University email facilities.

g. **"Spam"** means any electronic message that is sent without the express consent of the recipient(s). Spam is also used as the vehicle for the delivery of other online threats such as spyware, phishing, and malware.

5. Policy – Approved Use

5.1 The University provides an official University email account to all active students, faculty, and staff of the University. Email addresses are in the prescribed format of firstname.lastname@smu.ca. Modifications to naming format will be made by EIT if necessary to avoid confusion or duplication.

5.2 All students, staff, and faculty must:

a. activate an official University email account at the time they join the University;
b. use their official University email account when corresponding on University business or matters;
c. Regularly check their official University email account;
d. Never forward their official University email account to another email address that is not under the control of the University.

5.3 Students, faculty, and staff must provide and keep up to date an alternate email account (not smu.ca) only to facilitate account and password set-up or recovery.

5.4 **The official University email account must be used for students, faculty, and staff to conduct and communicate University business.** The use of personal email accounts or accounts other than the official University email account for the conduct of University business is prohibited. For greater certainty, all correspondence between students and faculty, between the University and faculty, staff, or students, must originate and be returned to a valid official University e-mail address. All emails to and from external parties that relate to business or activities conducted on behalf of the University or by a User in the capacity of employee or representative of the University must originate and be returned to valid official University e-mail address.

5.5 Users are expected to read, and shall be presumed to have received and read, all official

University email messages sent to official University email accounts.

5.6 All Users of official University email accounts must check their email account every two weeks at a minimum, as this is a primary method of communication used by the University to contact the community.

5.7 All Users must complete the Saint Mary's Cyber Security Awareness Training and observe responsible use of the technology in accordance with best practices prescribed by the Training and in accordance with this Policy.

5.8 All use of electronic communications and official University email accounts must be consistent with the University's Privacy Policy (12-003) and the Information Technology Policy (2-004).

6. Policy – Prohibited Uses

6.1 University email services and official University email accounts must not be used for any of the prohibited uses:

a. Intentional and unauthorized access to other people's email
b. Sending "Spam", chain letters, or any other type of unauthorized widespread distribution of unsolicited mail
c. For commercial activities or personal gain (except as specifically authorized by University policy)
d. For partisan political or lobbying activities
e. For any purpose that constitutes a violation of the Code of Student Conduct or any other University policy
f. Creation and use of a false or alias email address in order to impersonate another or send fraudulent communications
g. Use of email to transmit materials in a manner which violates copyright laws
h. for matters un-related to Saint Mary's University business.

6.2 In general, email is not appropriate for transmitting sensitive or confidential information, including personal information, unless an appropriate level of security matches its use for such purposes.

6.3 Alleged abuses of university email services should be directed to: itsecurity@smu.ca.

7. Privacy – University Access and Disclosure

7.1 The University will make reasonable efforts to maintain the integrity and effective operation of its email systems, but users are advised that those systems should not be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the University can assure neither the privacy of a User's use of the University's email resources nor the confidentiality of messages that may be created, transmitted, received, or stored using University email facilities.

7.2 E-mail created and received by Users is subject to the FOIPOP Act. Users must protect personal information in accordance with the Act and the Privacy Policy. Users are on notice that the University may be required to disclose e-mail correspondence in response to an Access to Information request under the FOIPOP Act.

7.3 Official University email accounts and the information contained on University email facilities are the property of the University, unless the information is the intellectual property of another person pursuant to an agreement (including a collective agreement), intellectual property law, or another University Policy.

7.4 Emails on University email facilities may constitute University Records as defined in the University's Records Management Policy and must therefore be managed in accordance with the requirements of that policy.

7.5 University EIT administrators control access to official University email accounts and

may perform security and privacy risk mitigation interventions with individual User accounts and/or the University as required.

7.6 The University does not routinely inspect, monitor, or disclose email without the User's consent. It may be necessary for the University to access a User's email account to maintain and improve the functioning of the email system. However, the University seeks to ensure that the contents of accounts that are accessed for such purpose will not be opened during this process.

7.7 Normally, a User's consent shall be sought by the University prior to any inspection, monitoring, or disclosure of University email records in the User's possession. The University shall permit the inspection, monitoring, or disclosure of email without the consent of the User only

a. when required by and consistent with law
b. when there is a reasonable apprehension that violations of law or of University policies have taken place
c. under time-dependent, critical operational circumstances where there is a high probability that failure to act could result in significant bodily harm, significant property loss or damage, significant liability to the University or members of the University community, or significant risk of hampering the ability of the University to meet its teaching obligations
d. when an employee or former employee is unavailable for a significant period and is in possession of information that is required for the University to meet its administrative obligations.
e. The inspection, monitoring or disclosure of student emails will only be permitted under clauses (a & b).

7.8 When the contents of email must be inspected, monitored, or disclosed without the User's consent, the following shall apply:

a. AUTHORIZATION. Except in emergency circumstances (i.e., time-dependent, critical operational circumstances where there is a high probability that failure to act could result in significant bodily harm, significant property loss or damage, or significant liability to the University or members of the University community), such actions must be authorized in advance and in writing by the Vice President, Finance and Administration or the Senior Director Legal Services. This authority may only be re-delegated to the President. Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation. In emergency circumstances, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay.
b. NOTIFICATION AND RECOURSE. The responsible authority shall, at the earliest possible opportunity that is lawful, notify the affected individual of the action(s) taken, the reasons for the action(s) taken, and the mechanisms available for recourse if the individual affected believes that actions taken were in violation of this Policy.

8. **Deactivation**

8.1 Official University email accounts will be deactivated based on the following timelines:

a. Students-4 months after the completion of their last enrolled class or convocation, whichever is later.
b. Faculty- upon termination of their appointment.
c. Staff and contractors- upon termination of their contract.

9. Relevant Legislation

9.1 FOIPOP Act.
9.2 Personal Health Information Protection Act (Nova Scotia)
9.3 Personal Information International Disclosure Protection Act (Nova Scotia)

10. Related Policies, Procedures & Documents

10.1 The following policies are related to this Policy and should be referred to as required for interpretation or understanding:
   a. Policy on Information Technology (2-2004)
   b. Privacy Policy (12-003)
   c. Records Management Policy (TBD)

Related Procedures: Records Retention Schedule