Carleton UNIVERSITY
Canada's Capital University

Policy Name:	Email (Electronic Mail) Use
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Senior Management Committee
Date of Original Policy:	April 2016
Last Updated:	October 2018
Mandatory Revision Date:	October 2023
Contact:	Assistant Vice-President (ITS) & Chief Information Officer

Policy:
The provision and operation of email services provided by the University must be performed in a consistent and secure manner that supports the business needs of the University.

Purpose:
This Policy defines the University's position on the provisioning, operation, use and decommissioning of email services at Carleton University.

Scope:
This Policy applies to:

- All email systems and services provided or owned by Carleton University
- All holders and users of University email services
- All University business conducted by email regardless of location, service provider or system ownership

Procedures:

Assignment of Email Accounts

Students
Carleton University students are assigned an email address at the time of admission to a course of study and retain it for life.

Faculty
Faculty are assigned an email address at time of engagement with Carleton University. Upon voluntary departure or retirement, all instructors, librarians, full professors , associate professors, assistant professors, adjunct professors and adjunct research professors retain email service for life.

Staff
Staff are assigned an email address at time of employment with Carleton University. Upon departure or retirement from Carleton, staff do not retain their email service.

Other Employee Types
Other employees include Contractors, Contract Instructors, Researchers, Post Doctorate, and any other employee that is not a continuing employee do not retain provisioned email services post-employment.

De-provision of Email Accounts

Email accounts which have not been accessed for three years, and which are not forwarded, will be deleted.

Terminated faculty and staff lose email service at the time of termination.

Ownership

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. 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) .

Situations may occur in which it may be necessary for the University to access an email account. Accordingly, the University reserves the right to examine or access any email account where the University, in its sole discretion, determines that it has reason to do so. Without limiting the University's discretion in this regard, such situations include but are not limited to: leave of any type, investigation of a complaint, allegation of usage that contravenes existing laws, policies, or guidelines, criminal or legal investigation, freedom of information requests or where necessary to carry out urgent operational requirements during an employee's absence when alternative arrangements have not been made. In support of these requirements, access to emails may extend to personal email accounts used for University business; as such it is strongly encouraged that only Carleton University provisioned email systems are used for business purposes.

At such time as it becomes necessary to access an email account under any of the circumstances stated above, permission must be granted by either the Assistant VP (Human Resources), the General Counsel, or associated delegates.

Acceptable Use

While acceptable use of IT resources falls user the University's Acceptable Use of Information Technology Policy, the following provides additional usage restrictions applicable to the use of Email.

Representation:
Email users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Carleton University or any unit of the University unless authorized to do so. Where necessary, an explicit disclaimer must be included such as, "These statements are my own and do not reflect the views or opinions of Carleton University."

Personal Use:

Carleton University email services may be used for personal purposes provided that, in addition to the constraints and conditions in this Policy and, such use does not:

- Directly or indirectly interfere with the University operation of computing facilities;
- Burden the University with noticeable incremental cost;
- Interfere with the email user's employment or other obligations to the University;
- Serve as a vehicle for personal profit and/or financial gain.
- Become excessive and does not interfere with proper performance of that person's duties.

Users should assess the implications of using University email services for personal purposes as such email may constitute an official record and be subject to FIPPA.

Prohibited Use of Email

Email must not be used to:

- Display or promote pornographic or offensive or obscene material;
- Promote violence, or the use of weapons, alcohol or illegal drugs;
- Send abusive or threatening language or imagery that targets individuals or groups;
- Conduct personalized attacks, harassment or cyber-bullying;
- Ridicule or promote stereotypes, discrimination, intolerance or hostility towards any race, sex, colour, ancestry, place of origin, ethnic origin, creed, marital status, gender identity, gender expression, family status, sexual orientation, age, disability, citizenship or any other prohibited ground of discrimination;
- Publish information intended to cause harm or which would reasonably be known to cause harm
- Send or forward chain letters;
- Send large attachments in mass mailings;
- Exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited email; i.e., spam;
- Resend the same email repeatedly to one or more recipients to interfere with the recipient's use of email; i.e., letter-bomb; and
- Introduce or intentionally propagate any computer code designed to self-replicate, damage or otherwise hinder the performance of any information technology or cause the compromise of sensitive or confidential information; i.e., viruses, trojans, worms.

<u>Academic Freedom</u>:
Academic freedom applies to faculty members in carrying out their responsibilities of teaching and research. The pursuit and publication of controversial research material and the study and teaching of material with controversial and even offensive content in the context of conscientious, professional instruction in the University are protected within academic freedom. However, it carries with it the duty to use that freedom in a manner consistent with ethical guidelines, human rights law, and the scholarly obligation to base research and teaching on an honest search for knowledge. It may also be circumscribed by civil and criminal law – see Carleton University's Human Rights Policies and Procedures.

Privacy of Content

While the University respects the reasonable privacy of emails stored or distributed on its servers and networks, there is no guarantee of privacy. University provided email may be accessed at any time under such circumstances as stated in this Policy.

The following guidance is available to assist users in making informed decisions when using email:

- Email messages can be easily forwarded to others
- Messages with confidential or sensitive information may traverse the Internet unencrypted and stored unencrypted as there is no assurance that encryption will be used end-to-end; when dealing with confidential or sensitive information alternate means of securing the information must be taken
- Email messages may exit Canada and traverse the United States depending on Internet service provider peering arrangements
- A reply to a message from a mailing list that you expect to go only to the originator can be circulated to all subscribers of the mailing list
- A message you have deleted can still persist on backup facilities and thus be subject to disclosure at a later time
- Email users should use common sense and good judgment to choose content and recipients of emails, especially with regards to confidential and proprietary information
- Email may constitute a University record, subject to disclosure under Canadian and provincial laws, or as a result of litigation
- The content of any email system, regardless of where it is stored, is subject to legislation such as the Canadian Anti-Terrorism Act and the US Patriot Act

Security

External email coming into University mail servers, as well as outgoing email from the University, must be scanned for the existence of various forms of malware, e.g. viruses, spyware, etc. Filtering against SPAM email must also be performed.

Scanning and SPAM filtering are affective tools, however, they are not foolproof and may let unwanted emails pass. As a result, the following guidance is provided:

- Users may still receive offensive email
- The apparent sender may not be the actual sender. when in doubt one should check with the purported sender to validate the authorship or authenticity of the message
- Legitimate messages could be blocked inadvertently
- Users should not respond to requests for personal identity information
- Users should be wary of opening email attachments from individuals they do not know as this is a common mechanism to compromise computer security

To further protect the University community, measures must be taken to reduce the number of emails that come into the University pretending to be from the @carleton.ca email domain. To accomplish this, all third party services used for email communications must:

- Have a formal security assessment performed
- Have a Privacy Impact Assessment performed
- Have an appropriate contract governing the implementation and use of the service

Retention

Electronic documents have the same legal status as paper documents. It is the responsibility of individual users to retain, manage, and archive email files in accordance with the University Corporate Records and Archives Policy and as per departmental directives and practices. The University does not operate an email archival facility.

Privacy Legislation

The provision and support of email services must be done in a manner that is fully compliant with the Freedom of Information and Protection of Privacy Act (FIPPA), an Ontario statute; and the Personal Information Protection and Electronic Documents Act, Canada (PIPEDA), a federal statute. The communication of personal information on the web must comply with the applicable provisions of FIPPA and PIPEDA. Inquiries regarding privacy and this statement are to be directed to the Privacy Office.

Compliance

Non-compliance with this Policy may result in disciplinary action and/or the termination of a user's access to email service.

Roles and Responsibilities

All providers of email services must:

- Ensure that the mail services support access to emails in the University's performance of investigations and fulfillment of Access to Information Requests
- Ensure that the mail services provide basic security services that include scanning of emails for malicious payloads and blocking of SPAM messages
- Retain emails for a minimum period of two years in support of investigations and Access to Information requests, even after user access is removed (ex: in the case of terminations, of staff departures where email accounts are not for life) or the mail server is decommissioned

Information Technology Services must:

- Perform security assessments on third party services in support of the Cloud Computing Policy

The Carleton University Privacy Office is responsible for:

- Performing Privacy Impact Assessments in support of the Cloud Computing Policy

The Department of University Communications must:

- Approve the use of third party service providers specifically involved in the issuance of communications via email services

Contacts: Assistant Vice-President (ITS) & Chief Information Officer

Links to Related Policies:

http://www.carleton.ca/secretariat/policies/

- Acceptable Use Policy for Information Technology
- Commercial Activities Policy
- Cloud Computing Security
- Corporate Records and Archives Policy

http://www.carleton.ca/privacy/policies/

- Carleton's Privacy Policies

http://www.carleton.ca/equity/human-rights/policy/

- Human Rights Policies and Procedures

http://www.carleton.ca/secretariat/policies/corporate-records-and-archives-policy/

- Corporate Records and Archives Policy

https://www.ipc.on.ca/english/decisions-and-resolutions/The-Acts/

- FIPPA (Freedom of Information and Protection of Privacy Act, Ontario)

https://www.priv.gc.ca/leg_c/leg_c_p_e.asp

- PIPEDA (Personal Information Protection and Electronic Documents Act, Canada)