Policy Name:	Acceptable Use of Information Technology and Email
Originating/Responsible Department:	Information Technology Services (ITS)
Approval Authority:	Senior Management Committee
Date of Original Policy:	November 2023
Last Updated:	November 2023
Mandatory Revision Date:	November 2028
Contact:	Associate Vice-President Information Technology Services and Chief Information Officer

Policy Statement:
Carleton University provides Information Technology (IT) resources, including email where appropriate, to the campus community of students, faculty, staff, contractors, visitors, alumni and retirees. Provision of access to these resources requires users to act responsibly to ensure that all IT resources, as well as external systems accessed from the Carleton University network are not abused or used for inappropriate or illegal activities.

Purpose:
To ensure that reasonable steps are taken to protect Carleton University IT resources from malicious activity and inappropriate use, and that Carleton's use of the internet does not adversely affect other organizations or individuals. This Policy defines the University's position on the provisioning, operation, use and decommissioning of IT resources at Carleton University.

Scope:
This Policy applies to all IT resources of the university including networks, email systems, information systems, applications and information assets. The Policy applies to all individuals and organizations that use Carleton University IT resources from on campus or off campus, and to all IT resources provided by or on behalf of Carleton University.

Interpretation:
1. This Policy shall read in conjunction with other applicable policies, agreements and applicable law that may, in certain circumstances, govern data protection risk management matters, including collective agreements, IT and information security policies, agreements and records management and archives policies and procedures.
2. This Policy shall be read in conjunction with any policies, directives, guidelines and procedures that are established concerning data protection.

Procedure:
Carleton University provides access to IT resources with the expectation that these resources are used in a responsible manner and in compliance with applicable polices, agreements and applicable law. Appropriate use of the Carleton University computing resources includes but is not limited to:

- Use of IT resources for the purpose for which they are intended;
- Adherence to the rules governing the use of IT resources as established by Carleton University;
- Respect for the property of others;
- Reporting any occurrences of misuse of IT resources to university authorities;
- Consideration of other persons using shared IT resources and facilities; e.g., student labs;
- Maintaining the confidentiality of passwords, authentication services, other account information and data provided to users;
  Adhering to software licence agreements, university policies and law as applicable.

Inappropriate use of the Carleton University IT resources includes, but is not limited to:

- Unauthorized access, alteration, destruction, removal and/or disclosure of data, information, records, equipment, software or other IT resources;
- Use of Carleton University IT resources to gain unauthorized access to, or deliberately impair the functioning of any computer system or IT resource;
- Violation of software licence agreements and University policies when using software on IT resources;
- Deliberate over-extension of the resources of a system or interference with the normal processing of a system; e.g., deliberate attempts to make an IT resource unavailable to its intended users;
- Unauthorized disclosure of confidential passwords and/or access devices or information for accounts, equipment and telephone voice mail;
- Development of any third-party website or service that requires users to submit their Carleton username/password for access, without formal consent and approval of Carleton University;
- Unauthorized use of university facilities and resources for commercial purposes or personal gain;
- Use of IT resources to facilitate propagation of hate material or literature;
- Use of IT resources to facilitate any form of harassment;
- Theft or misuse of resources;
- Malicious or unethical use, including inappropriate, malicious or unethical use of social media;
- The creation of or distribution of malicious software including but not limited to viruses, worms, Trojans, spyware, rootkits and adware, etc., that affects the confidentiality, integrity or availability of University IT systems or data;
- Any use that violates any applicable law or regulation;
- The impairment, avoidance or alteration of IT security controls; and
- Testing or attempting to compromise university IT resources without the written approval of the system owner.

Legitimacy of Use and Ownership

In the university environment, there may be legitimate reasons for conducting some activities that would typically be considered “inappropriate use” for legitimate research purposes. In the event that a user has a legitimate reason to use IT resources in a manner that violates this Policy, they must obtain prior written approval from the department responsible for the management of the IT resources prior to using the resources for these purposes and have an approved research ethics protocol.

Electronic records, including email, pertaining to university business have the same legal status as analog records, and are subject to all regulations and policies governing University data, information and 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).

Situations may occur in which it may be necessary for the University to access IT resources assigned to an individual faculty or staff member. 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 only Carleton University provisioned email systems are to be used for University 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 Vice President (Human Resources), the General Counsel, or their associated delegates.

Assignment and Use of Email

Email accounts are assigned and deprovisioned as outlined in Schedule 1.

The following are additional usage restrictions applicable to the use of Email.

Representation:

Email users must not represent or otherwise make 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 reasonably used for personal purposes provided that, in addition to the constraints and conditions in this Policy and applicable law, 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 or to conduct non-university related commercial activities;
- Is not excessive and does not interfere or conflict with the proper performance of that person's duties;
- Create a cyber security risk, breach agreements, policies or applicable law.

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

In addition, email shall 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, phishing;
- Resend the same email repeatedly to one or more recipients to interfere with the recipient's use of email; i.e., spam;
- 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;
- Violate policies, agreements or applicable law; and
- in another manner that may negatively impact the university's reputation.

Privacy
The provision, support and use of IT resources must be done in a manner that is fully compliant with all applicable law including but not limited to the *Freedom of Information and Protection of Privacy Act* (FIPPA), and the *Personal Information Protection and Electronic Documents Act*, Canada (PIPEDA). The communication of personal information on all IT resources must comply with the applicable provisions of FIPPA and PIPEDA. Inquiries regarding privacy and this statement are to be directed to the Privacy Office. Users should expect and understand that there is no guarantee of privacy when using Carleton IT or email resources.

Carleton University reserves the right to monitor the use of resources provided and/or managed by the university for the purposes of determining adherence to policies and applicable law. Access to IT resources may be required in support of any number of reasons including but not limited to: troubleshooting and technical support, leave of any type, security, criminal, employment or legal investigation and freedom of information requests.

Roles and Responsibilities:
All individuals and organizations that use Carleton University IT resources from on campus or off campus are responsible for ensuring their use of Carleton University IT resources complies with this policy.

ITS is responsible for:

- Technology support for the implementation of this policy;
- The provision of enterprise email services per schedule 1;

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

Contacts:

Associate Vice-President (Information Technology Services) and Chief Information Officer

Links to related Policies:

- Student Rights and Responsibilities Policy
- Human Rights Policy and Procedures
- Access to Information and Privacy
- Data Protection and Risk Management
- Information Technology Procurement
- University Information Technology (IT) Security
- Electronic Monitoring
- Corporate Records and Archives

Schedule 1: Assignment and De-provisioning of Email Accounts

Assignment of Email Accounts

Students
Carleton University students are assigned an email address at the time of admission to a regular program or course of study and retain it for life subject to compliance with University policies and applicable license agreements and law.

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 subject to compliance with University policies and applicable license agreements and law.

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. A Post-Doctorate employee may submit a written request to the Office of the Deputy Provost to maintain access to their Carleton email account for a maximum of twelve (12) months after the conclusion of their Postdoctoral Fellow appointment.

Contract Instructors retain access to email services two (2) years from the completion of their contract with the university.

De-provision of Email Accounts
Any email accounts which have not been accessed for three years will be deleted. Terminated faculty and staff lose email service at the time of termination**.**