POLICY NAME	**POLICY ON THE RESPONSIBLE USE OF MCGILL INFORMATION TECHNOLOGY RESOURCES**
Approving Body	Board of Governors
Initial Approval Date	March 24, 2010 - Senate April 12, 2010 - Board of Governors
Date of last review	May 21, 2020 – Board of Governors
Date of next review	May 2025
Executive Sponsor	Vice-President (Administration and Finance)

Related Documents	"IT Documents" accessible at http://kb.mcgill.ca/ and https://www.mcgill.ca/it/

PURPOSE AND SCOPE

Purpose

The purpose of the Policy on the Responsible Use of McGill Information Technology Resources ("Policy") is to ensure that McGill information technology resources ("McGill IT Resources") are used to advance the mission of McGill University ("University") and to support any related administrative, financial and operational activities. To this effect, the Policy aims to safeguard the Security of all McGill IT Resources, by establishing the responsibilities of the University and of the University community in the use of all McGill IT Resources.

Scope

This Policy governs the use of all McGill IT Resources and applies to all members of the University community, including faculty, staff, students, retirees, alumni, appointees, consultants, guests or other individuals who have been granted permission to use McGill IT Resources.

CONTENT

1. Definitions

For the purposes of this Policy, capitalized words have the following meaning:

1.1. "Authorized User" means a member of the McGill University community and includes faculty, staff, students, retirees, alumni, appointees, consultants, guests or other individuals who have been granted permission to access certain data or systems that are part of McGill IT Resources by virtue of their role and responsibilities.

1.2. “Availability” means the assurance of timely and reliable access to McGill IT Resources for their intended use.

1.3. “Broadcast Communications” means email or other electronic communications transmitted through McGill IT Resources to a collection of electronic addresses, including, but not limited to, Yammer, listservs, distribution lists and class lists.

1.4. “Confidentiality” means the assurance that IT Credentials or Data can only be accessed by Authorized Users or authorized systems.

1.5. “Confidential Data” means information whose protection and use is mandated and governed by law, regulation, industry requirement, contract or any McGill regulation, policy or directive because of its sensitive nature, including, but not limited to, Personal Information.

1.6. “Data” means digital information stored in or transmitted through McGill IT Resources and includes documents, files, databases, emails and multimedia.

1.7. “Integrity” means the assurance of the accuracy and consistency of Data and that Data is not altered by unauthorized users.

1.8. “IT Credentials” means a proof of identity used to control access to McGill IT Resources, including, but not limited to, usernames, passwords, biometrics, digital certificates and key cards.

1.9. “IT Documents” means the guidelines, standards and directives related to this Policy appearing in the IT Knowledge Base or IT Services website.

1.10. “IT Services” means the McGill unit that delivers information technology services to the McGill community and reports to the CIO (Chief Information Officer).

1.11. “McGill email address” means an email address issued by IT Services to an Authorized User, according to the official format as defined by IT Services.

1.12. “McGill IT Resources” means all university-owned or provisioned IT assets. This includes, but is not limited to, Data, cloud services, software, hardware, voice communications systems, internet of things (IoT) and devices, and the services that make use of any of these IT resources.

1.13. “McGill-Sponsored Public Website” means a website that is hosted on McGill IT Resources and is accessible by any member of the public with a web browser and access to the Internet.

1.14. “Non-McGill Use”, also known as personal use, means usage that is not for the purpose of advancing the mission of the University and supporting related administrative, financial and operational activities or that has not been otherwise authorized.

1.15. “Personal Information” means information, which relates to a natural person and allows that person to be identified, as provided for in applicable privacy legislation.

1.16. "Security" means the protection of Confidentiality, Integrity and Availability of McGill IT Resources.

1.17. "System Administrator" means an individual responsible through position description or position responsibilities for establishing and maintaining a computer system or network.

1.18. "University Network" means the wired and wireless network for Data, voice and video under the control of IT Services.

2. Principles

2.1. McGill IT Resources are provided to Authorized Users only for the purpose of advancing the mission of the University and in order to support related administrative, financial and operational activities.

2.2. Authorized Users shall use McGill IT Resources, for the purposes provided in section 2.1, and in a responsible, ethical and lawful manner, in accordance with University policies, directives and procedures, and other relevant University standards and guidelines, and in compliance with applicable laws and regulations as well as, in certain circumstances, University contracts and agreements.

2.3. Authorized Users have a reasonable expectation of privacy in their use of McGill IT Resources.

2.4. Authorized Users shall take reasonable and prudent steps to protect the Security and ensure the Confidentiality, Integrity and Availability of McGill IT Resources.

2.5. Ability to access and use McGill IT Resources does not, by itself, imply authorization to do so.

2.6. Authorized Users shall respect the intellectual property rights of others.

2.7. Authorized Users must use technology in accordance with IT Documents and best practices in the University.

3. IT Credentials

3.1. Authorized Users shall not share their personal IT Credentials.

3.2. If it is essential that an IT Credential be shared and delegation is not supported by the application, the Authorized User shall use an IT Credential that is intended for that specific purpose, such as a resource account or a shared mailbox.

3.3. When using McGill IT Resources, Authorized Users shall properly identify themselves using their IT Credentials in applications, services or connections. An Authorized User shall not impersonate another person, except for Authorized Users that have been explicitly granted impersonation privileges in certain applications for the purposes of testing or configuration.

3.4. Notwithstanding section 3.3, Authorized Users may remain anonymous for legitimate purposes such as certain surveys.

4. Security

4.1. Authorized Users shall not use McGill IT Resources in any way that may compromise the Security of McGill IT Resources or put the University at risk.

4.2. Authorized Users shall report suspected actual or potential threats to the Security of McGill IT Resources in accordance with relevant IT Services' directives and protocols and shall cooperate with investigations of possible breaches.

4.3. Authorized Users shall not attempt to circumvent IT security controls without the prior written approval of ITS Services (IT Security).

5. Data

5.1. Subject to section 5.2, Confidential Data shall only be accessed by or with the consent of Authorized Users or by other individuals with a legitimate need to have access and who have been granted access by an Authorized User. The Confidentiality of the Data accessed shall be preserved and the Data shall be used solely for the purposes for which it was accessed.

5.2. Notwithstanding section 2.3, access to Authorized User Data may be provided to a designated University administrator with a legitimate interest in and responsibility for the matter in the following cases:

(i) For continued operation of the University where the Authorized User whose Data are accessed is unavailable or no longer at McGill.

(ii) To investigate breaches of University policies or regulations where reasonable grounds exist to believe that a breach has occurred.

(iii) Where permitted by law.

5.3. At the earliest stages of consideration regarding the use of an information technology vendor for storage, processing or transmission of institutional Data, an Authorized User shall consult Procurement Services for guidance. Procurement Services will consult with IT Services and Legal Services where required.

6. Email and Broadcast Communications

6.1. Email messages must comply with standards and laws concerning privacy, and retention and destruction of documents. Consequently, faculty and staff Authorized Users shall seek authorization from the CIO or delegate, to:

(i) systematically/automatically forward/redirect their email to external mail servers

or

(ii) configure to download/pull all their email to external mail servers.

Manual forwarding/redirecting of select email messages is permitted, subject to other provisions of McGill policies and regulations.

6.2. Authorized Users are permitted to send Broadcast Communications if the content of the message is related to McGill's teaching, research or administrative functions and if

(i) the Authorized User is permitted to send the broadcast by virtue of their function or

(ii) the Authorized User is permitted to send the broadcast to individuals that have knowingly subscribed.

6.3. Authorized Users who are part of administrative units shall send Broadcast Communications in accordance with IT Documents for Security best practices, formats and attachments.

7. Public Websites

7.1. An Authorized User who publishes information on a McGill-Sponsored Public Website shall ensure that the content does not violate this Policy, any other University policy, directive or procedure or any applicable laws or regulations.

7.2. No external or commercial advertising shall appear in any McGill-Sponsored Public Website without the prior written approval of Communications and External Relations who shall consult the appropriate senior administrator where required. Notwithstanding this provision, sponsorship of University activities, including, but not restricted to, academic conferences, symposia and the like, may be recognized on the appropriate McGill Websites.

7.3. All McGill Websites shall be developed in conformity with the McGill digital communication governance framework, which addresses Web standards and standards for security, naming conventions, accessibility, visual and branding identity.

7.4. Domain names that include the word "McGill" shall not be purchased or registered by individual units or McGill employees without the approval of Communications and External Relations.

7.5. Analytics and user tracking have ethical and privacy implications. Data collections for analytics and user research is limited to interactions around links, buttons and page elements. Personal Information or Confidential Data can only be collected in accordance with applicable laws.

8. Network

8.1. The University may limit or block internet traffic, where the traffic exposes the University or Authorized Users to threats to Security or where it is necessary to ensure the Confidentiality, Integrity or Availability of McGill IT Resources.

8.2. Authorized Users shall not extend or share the University Network with public or other persons

unless written authorization has been obtained from IT Services.

8.3. Authorized Users shall not connect any network devices (including switches, routers, wireless access points, VPNs and firewalls) to the University Network without prior written approval of IT Services. Standard exceptions outlined in IT Documents do not require additional approval.

8.4. Authorized Users may only connect devices to the University Network that comply with IT Documents related to cybersecurity.

9. System Administration

9.1. All McGill IT Resources shall have a duly appointed System Administrator. Where an academic unit has not made other arrangements, researchers or their delegates are System Administrators of the research systems they control.

9.2. System Administrators shall respect the policies, directives, standards and procedures established by the University, and configure and manage systems in accordance with best practices in the University.

9.3. Notwithstanding due regard to users' privacy, System Administrators may routinely monitor or access accounts or use software and hardware tools (including surveillance or monitoring tools, cookies, audit trails and logs, backups and archives), to track or preserve activity on the system. They shall only use such Data within their legitimate authority and will treat any Data accessed for this purpose as confidential.

9.4. Authorized Users using McGill IT Resources in breach of McGill's policies and procedures or in excess of their authority are subject to having their activities monitored and recorded by System Administrators. In the course of monitoring individuals improperly using McGill IT Resources, or in the course of McGill IT Resources maintenance, the activities of Authorized Users could also be monitored.

10. Non-McGill Use

10.1. The University does not warrant any service or Confidentiality levels for Non-McGill Use of McGill IT Resources.

10.2. McGill University reserves the right to limit or stop Non-McGill Use where the use exposes the University to risk.

11. Enforcement

11.1. A violation of the provisions of this Policy may constitute a disciplinary offence and, where appropriate, shall be dealt with under the regulations, policies, code or collective agreement to which the Authorized User is subject.

11.2. Any individual who has reasonable cause to believe that there has been a breach of this Policy shall report the matter to the CIO.

11.3. A report identifying the type of access granted under 5.2 (Data) shall be prepared by the unit heads or their delegates and provided to the CIO upon request. The CIO shall in turn report to the Vice-President (Administration and Finance) on such activity. The report shall contain aggregated information and shall not identify individuals by name.

AUTHORITY TO APPROVE PROCEDURES

The Vice-President (Administration and Finance) or his delegate has the authority to establish and amend procedures necessary for the purpose of implementing this Policy.

REVIEW

This revised Policy will come into force on May 21, 2020.

This Policy will be reviewed every five years following its last review date.

Legislative History:

Approved:		
Senate	March 24, 2010	Minute 11B4
Board of Governors	April 12, 2010	Minute 10.1
Revised:		
Board of Governors	April 12, 2010	Minute 11.1.3