McGill **Memorandum**

Office of the Provost
James Building, Room 506

TO: Senate

FROM: Professor Anthony C. Masi, Provost
Chair, Academic Policy Committee

SUBJECT: Responsible Use of McGill Information Technology Resources

DATE: January 27, 2010 (for Senate meeting on February 10, 2010)

DOCUMENT #: D09-42

ACTION REQUIRED: □ INFORMATION □ DISCUSSION ☒ APPROVAL / DECISION

ISSUE:

Since 1994, the University has had a Code of Conduct for Users of McGill Computing Facilities and accompanying Computing Facilities Management Guidelines. These documents have served the University well in the past, but have been superseded by the evolution of information technology and the pervasiveness of its use in all aspects of the University, including the creation of the world wide web, the wide use of e-mail and other collaboration software tools, and the implementation of enterprise-wide, interoperable databases. Furthermore, delivery of information technology services has matured, and McGill systems managers have applied a myriad of industry best practices and standard procedures to University systems.

Specific issues that have been raised

In addition to the need for an update to address technological change, other concerns have been raised to the office of the Chief Information Officer, as well as at Senate. These include:

- the circumstances under which e-mail or computer files are accessed,
- authority to ensure that material posted on the web conforms with University policy,
- the acceptability of having web sites with user comments and contributions posted,
- the provisions to ensure that research data are maintained in a confidential manner
- whether or not to block certain web sites from being viewed on campus,

- questions related to the use of the McGill name in URLs.

The proposed policy addresses these issues. It refers to current IT issues and has been informed by similar documents issued by universities across North America. It would replace the Code of Conduct for Users of McGill Computing Facilities and the accompanying Computing Facilities Management Guidelines. The proposed policy would co-exist with the Code of Student Conduct and Disciplinary Procedures and with other University policies on campus.

BACKGROUND & RATIONALE:

See above.

MOTION OR RESOLUTION FOR APPROVAL:

Be it resolved
that Senate approve the proposed Policy on Responsible Use of McGill Information Technology Resources and recommend to the Board of Governors that it be approved.

Be it further resolved
that the new Policy, if approved, take effect immediately and that the Code of Conduct for Users of McGill Computing Facilities and the McGill Computing Facilities Management Guidelines cease to be effective as of the same date.

PRIOR CONSULTATION/ APPROVAL:

Consultations:
August 21, 2009 –Circulated IT Directors and Associate Directors
September 14, 2009 – Circulated to Academic Planning Group (APG) members for review
September 21, 2009 – APG
October 5 – APG (continuation)
October 14, 2009 – Deans' Working Group meeting
November 5, 2009 – Academic Planning Committee (APC)
November 5, 2009 – Circulated to Student Advisory Council on IT
November 18, 2009 – P7
November 18, 2009 – Enrolment and Student Affairs Advisory Committee (ESAAC)
November 26, 2009 – APC
December 2, 2009 – Senate
December 8, 2009 – Subcommittee on Teaching and Learning (SCTL)
December 9, 2009 – Research Advisory Committee (RAC)
January 11, 2010 – APG

Approvals:
January 21, 2010 – APC approval

NEXT STEPS:

Submission to the Board of Governors
Implementation of the Policy on Responsible Use of McGill IT Resources

APPENDICES:

Responsible Use of McGill Information Technology Resources Policy
(25th January 2010)

January 25, 2010

Responsible Use of McGill Information Technology Resources

This policy replaces the following:

Code of Conduct for Users of McGill Computing Facilities
McGill Computing Facilities Management Guidelines

Preamble

McGill information technology resources (hereafter McGill IT Resources) serve the University's mission of the advancement of learning through teaching, scholarship and service to society. The University provides an atmosphere that encourages access to knowledge and sharing of information. The University is responsible for ensuring the effective and reliable operation of our systems and protection of our information technology resources. This policy outlines the responsibilities of the University and members of the University community in the use of McGill IT Resources.

1. Definitions:

For the purposes of this Policy:

1.1. "Authorized User" is a member of the McGill University community who is an employee, student, alumni, appointee or other individual who has been granted permission, by virtue of the individual's role and responsibilities, to access certain data or systems that are part of McGill IT Resources.

1.2. "Availability" means the accessibility of McGill IT Resources for their intended use.

1.3. "Broadcast Communications" means e-mail or other electronic communications transmitted through McGill IT Resources to a group, including, but not limited to, listservs, distribution lists, and class lists.

1.4. "CIO" means the Chief Information Officer.

1.5. "Confidentiality" means the non-disclosure of Credentials or Data to unauthorized individuals or systems.

1.6. "Confidential Data" means Data that is of a private, proprietary or otherwise sensitive nature, including, but not limited to, Personal Information.

1.7. “Credentials” includes usernames, access codes, account numbers, passwords, PINs, tokens or other authentication which have been assigned to Authorized Users to access McGill IT Resources.

1.8. “Data” means information stored in or transmitted through McGill IT Resources, including documents, files, databases, e-mails and multimedia.

1.9. “Integrity” means protection from modification of Data by unauthorized individuals.

1.10. “IT Services” means the McGill units that deliver information technology services on campus and report to the CIO.

1.11. “McGill e-mail address” means an e-mail address issued by IT Services to an Authorized User, according to the official format as defined by IT Services. For example, the McGill e-mail address for staff members is usually first.last@mcgill.ca, and for students and alumni, first.last@mail.mcgill.ca.

1.12. “McGill IT Resources” means all Data, software, hardware, communications systems, storage systems, networks and devices connected to or making use of the University Network, regardless of who administers them.

1.13. “Non-McGill Use” means use that is not in accordance with section 2.1.

1.14. “Personal Information” means information concerning a natural person that allows the person to be identified as provided for in applicable Canadian and Quebec privacy legislation.

1.15. “Security” means the protection of Data and systems from breaches to or of Availability, Confidentiality or Integrity of McGill IT Resources.

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

1.17. “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 serve the teaching, research and administrative purposes of the University.

2.2. Authorized Users shall use McGill IT Resources in an ethical, responsible and lawful manner, in accordance with University policies.

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

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

2.5. Authorized Users shall only access McGill IT Resources in accordance with McGill's policies and procedures. Ability to access McGill IT Resources does not, by itself, imply authorization to do so.

2.6. Authorized Users shall respect the intellectual property, including but not limited to, trademarks and copyrights, of owners of software and Data stored in or transmitted through McGill IT Resources, including library and archival resources.

3. Credentials

3.1. Authorized Users shall not share their personal Credentials with other individuals. Where it is essential that an account be shared and delegation is not supported by the application, the Authorized User shall use a Credential that is intended for that specific purpose.

3.2. Authorized Users shall properly identify themselves in applications, services, or connections that use McGill IT Resources. An Authorized User shall not impersonate another person.

3.3. Notwithstanding sections 3.1 and 3.2, Authorized Users may participate in a survey or evaluation process, where anonymity is a characteristic of the survey.

4. Security

4.1. Authorized Users shall take the measures necessary to protect the Security of McGill IT Resources and shall comply with University policies and procedures concerning data protection and records management.

4.2. Authorized Users shall not use McGill IT Resources for any purpose that puts the University at risk of compromising Security.

4.3. Authorized Users shall comply with all University protocols for reporting threats to Security and shall cooperate with investigations of possible breaches.

4.4. Individuals 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 may also be monitored.

5. Data

5.1. Subject to section 5.2, Confidential Data shall only be accessed by Authorized Users or by other individuals with a legitimate need to have access who are 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 there exist reasonable grounds to believe that a breach has occurred.

(iii) Where permitted by law.

5.3. Before entrusting storage, processing or transmission of Personal Information to an information technology vendor controlled by a company or service outside Quebec, an Authorized User shall consult the CIO for guidance who will consult with senior administrators as appropriate.

6. E-mail and Broadcast Communications

6.1. E-mail services are provided to Authorized Users for the purpose of facilitating effective academic and administrative operations.

6.2. To ensure that e-mail records are managed according to University Data retention policies, all employees shall ensure that their McGill e-mail address forwards to a McGill e-mail server. Employees shall not configure their McGill e-mail to forward to a non-McGill e-mail address, without prior authorization from the CIO or delegate. Notwithstanding this provision, academic staff may forward their e-mail during sabbaticals to a non-McGill e-mail server, after they have assured themselves that the e-mail receives protections similar to those of university e-mail accounts.

6.3. Authorized Users shall send Broadcast Communications only if the content of the message is related to McGill's academic or administrative functions, and
(i) the individual is authorized to send the message by virtue of his or her function or

(ii) the broadcast is sent to a list that individuals have knowingly joined.

6.4. Authorized Users shall send Broadcast Communications in accordance with University standards for formats and attachments, such as pdf, as issued by IT Services.

7. Public Web Sites

7.1. An Authorized User who publishes information on a McGill-sponsored public web site shall ensure that the content conforms to University policies and procedures.

7.2. Where McGill sponsors a collaborative web site, such as blogs, wikis or social networks, the site shall conform to guidelines issued by the CIO.

7.3. No external or commercial advertising shall appear in any public McGill web site without the prior approval of the CIO who shall consult the appropriate senior administrator. Notwithstanding this provision, sponsorship of University activities, including, but not restricted to, academic conferences, symposia and the like, may be advertized on the appropriate McGill web sites.

7.4. McGill academic and administrative units shall host their administrative web site on the University's web publishing system in conformity with the McGill web publishing guidelines issued by IT Services.

7.5. Domain names that include the word "McGill" shall not be purchased or registered by individual units or McGill employees without the approval of the Secretary-General.

8. Network

8.1. IT Services shall not normally use technology to prevent an Authorized User of McGill IT Resources to access an external web site, where the computer has been configured to have access to the internet.

8.2. Notwithstanding section 8.1, the University shall moderate, filter, limit or block internet traffic, where it 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.

8.3. Authorized Users shall not extend or share the University Network with public or other persons beyond what has been authorized by IT Services.

8.4. Authorized Users shall not connect any network devices or systems (including switches, routers, wireless access points, VPNs, and firewalls) to the University Network without prior approval of IT Services.

8.5. Authorized Users may only connect devices to the University Network that comply with University guidelines related to malware.

9. Systems 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 research systems that they control.

9.2. Systems Administrators shall respect the policies, procedures and protocols established by the University and configure and manage systems according to best practices in the University and in conformity with the provisions of this policy.

9.3. In the performance of their duties, Systems 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.

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. **Compliance**

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 Office of the CIO.

11.3. An annual report identifying the type of access granted by IT Services under Section 5 (Data) shall be prepared by the CIO or delegate and provided to the Provost. The annual report shall contain aggregated information, and shall not identify individuals by name.