ACADEMIC COUNCIL REPORT

SESSION: **ACTION REQUESTED:**

Public ☒ **Decision** ☐
Discussion/Direction ☒
Information ☐

Financial Impact ☐ **Yes** ☒ **No** **Included in Budget** ☐ **Yes** ☒ **No**

TO: **Academic Council**

DATE: **February 25, 2020**

PRESENTED BY: **Cheryl Foy, University Secretary and General Counsel**
Niall O'Halloran, Policy and Compliance Advisor

SUBJECT: **Draft Technology Use Policy for Consultation**

COMMITTEE/BOARD MANDATE:

- Academic Council has a role in the Policy Framework as a mandatory consultation body for all substantive amendments to existing Legal, Compliance and Governance Policies.
- We ask for your consideration of and comments on substantive amendments to the Technology Use Policy.

BACKGROUND/CONTEXT & RATIONALE:

- The University owns, maintains and manages Information Technology (IT) resources to support the educational, instructional, research and administrative activities of the University. The University's current Technology Use Policy was approved by the Board in May 2012.
- While university members are free to use IT resources in pursuit of their individual and collective academic and administrative goals, it is equally important that safeguards are in place to ensure that the information, equipment and networks remain reliable, robust and secure on an ongoing basis. This Policy sets out the acceptable and responsible use of IT resources in a manner that is consistent with Ontario Tech University's values of integrity and responsibility, honesty and accountability, and intellectual rigour.
- This policy sets out expectations for acceptable and unacceptable use, and clarifies the privacy expectations for university members who use IT resources. This policy may refer incidents to resolution processes outlined in the following policies that address unacceptable conduct at the university:
    - Harassment and Discrimination Policy and Procedures;

    - Workplace Violence, Harassment and Discrimination Policy and Procedures;
    - Student Sexual Violence Policy and Procedures;
    - Student Conduct Policy; and
    - Academic Integrity Policies (academic integrity regulations in the Graduate and Undergraduate Academic Calendars).
- This policy commits to and does not conflict with the rights of university members to academic freedom. Ownership and other rights in intellectual property created using IT resources is determined by the university's Intellectual Property Policy, not the Technology Use Policy. Where this policy may intersect with collective agreement(s), the terms of the collective agreement prevail, per s. 9.3 of the Policy Framework.

RESOURCES REQUIRED:

- N/A

IMPLICATIONS:

- N/A

ALIGNMENT WITH MISSION, VISION, VALUES & STRATEGIC PLAN:

- This policy supports the university's commitments to academic freedom and freedom of expression

ALTERNATIVES CONSIDERED:

- N/A

CONSULTATION:

- Ontario Tech Information Technology Services
- Academic Council (November 26, 2019)
- Senior Leadership Team
- Policy Advisory Committee
- Online Consultation
- Administrative Leadership Team
- Audit & Finance Committee
- Board of Governors

COMPLIANCE WITH POLICY/LEGISLATION:

- *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31
- *Canada's Anti-Spam Legislation*
- *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5

NEXT STEPS:

- Continue consultation and approval path outlined above

MOTION FOR CONSIDERATION:

- N/A

SUPPORTING REFERENCE MATERIALS:

- Draft Technology Use Policy
- Technology Use Policy (current approved version)

Classification Number	LCG 1109
Framework Category	Legal, Compliance and Governance
Approving Authority	Board of Governors
Policy Owner	Provost and Vice President, Academic
Approval Date	DRAFT FOR CONSULTATION
Review Date	
Supersedes	Technology Use Policy, May 2012

TECHNOLOGY USE POLICY

PURPOSE

1. The University owns, maintains and manages Information Technology (IT) resources to support the educational, instructional, research and administrative activities of the University.

2. While University Members are free to use these valuable resources in pursuit of their individual and collective academic and administrative goals, it is equally important that safeguards are in place to ensure that the information, equipment and networks remain compliant, reliable, robust and secure.

3. This Policy sets out the acceptable and responsible use of IT Resources in a manner that is consistent with Ontario Tech University's values of integrity and responsibility, honesty and accountability, and intellectual rigour.

4. Before University Members can access or use the University's IT Resources, University Members must:

4.1. review this Policy or a terms of use that fully complies with this policy, as well as other policies applicable to the type of user; and

4.2. accept the University's terms and conditions of use.

DEFINITIONS

5. For the purposes of this Policy the following definitions apply:

"Electronically-Stored Information" ("ESI") means University Members' [personal] electronic information, other than a University Record, that is created and communicated in digital form and which is accessible through IT Resources.

"Information Assetmeans a fixed unit of information recorded by electronic means that is considered a University Record under the Records Management Policy.

"Guest" means any individual that is not a volunteer, Employee, or Student who uses or attempts to use IT Resources. A Guest who accepts the University's terms and conditions of use is considered a University Member under this policy.

"IT Resources" are information technology resources provided by the University, whether on premises or hosted remotely. IT Resources include but are not limited to:

- networks, including wireless access services, wired networks, switching and routing, load balancers, firewalls, telecom equipment and cables, PBX and other network-related devices, equipment and services;
- servers;
- databases;
- business systems;
- student systems;
- learning management systems;
- websites;
- computers and computer systems, laptops, workstations, computer labs, mobile devices, including telephones, storage devices; and
- online collaborative tools including email, and social media sites (e.g., the University's Twitter, Facebook and YouTube accounts).

"University Member" means any individual who is:

- Employed by the University (**"Employee"**);
- Registered as a student, in accordance with the academic regulations of the University (**"Student"**);
- Holding an appointment with the University, including paid, unpaid and/or honorific appointments; and/or
- Otherwise subject to University policies by virtue of the requirements of a specific policy (e.g. Booking and Use of University Space) and/or the terms of an agreement or contract.

SCOPE AND AUTHORITY

6. This Policy applies to all University Members' use of IT Resources and all IT Resources. The use of personally-owned equipment that involves the use of IT Resources is also covered by this Policy.

7. The University is fully committed to promoting and advocating academic freedom. This policy does not limit academic freedom.

8. This Policy does not affect the intellectual property rights of University Members stored or transmitted using IT Resources. Intellectual property rights are governed by the University's Intellectual Property Policy.

9. The Provost and Vice-President, Academic or successor thereof, is the Policy Owner and is responsible for overseeing the implementation, administration and interpretation of this Policy.

POLICY

10. Authorized Use

10.1. University Members will:

a) Use only those IT Resources for which the University has given express authorization, and only for intended purpose(s);

b) Take all reasonable steps to avoid compromising the confidentiality, integrity, and availability of IT Resources;

c) Abide by applicable laws and regulations;

d) Abide by applicable University policies, and;

e) Respect the rights and privacy of other University Members and those outside of the University community.

10.2. University Members who fail to comply with this Policy will be subject to one or more of the consequences listed in Section 12.

10.3. The University reserves the right to limit or restrict a University Member's access to IT Resources based on:

a) institutional priorities;

b) financial considerations;

c) one or more violations of this Policy or other University policies;

d) contractual agreements; or

e) provincial or federal laws.

11. Reporting

11.1. University Members are responsible for guarding against misuse or abuse of IT Resources.

11.2. University Members will promptly report any known or suspected misuse of IT Resources or violation of this Policy in accordance with the Acceptable Use of Technology Procedures.

11.3. Procedures for receiving reports, investigating and resolving conduct in contravention of this Policy will be developed by [the Office of the Provost].

12. Specific Violations

12.1. Unauthorized Use. Violations of Section 9.1.a) include, but are not limited to:

a) using resources without specific authorization where specific authorization is required;

b) using another person's electronic identity;

c) accessing files, data or processes without authorization;

d) using IT Resources to hide a persons' actual identity;

e) using IT Resources to interfere with other systems or persons;

f) using IT Resources to harass or stalk another person or entity;

g) sending threats, "hoax" messages, chain letters, or phishing;

h) intercepting, monitoring, or retrieving any network communication without authorization; or

i) circumventing or attempting to circumvent security mechanisms.

12.2. Breach of Confidentiality, Integrity and Availability of IT Resources. Violations of Section 9.1.b) include, but are not limited to:

a) obtaining or using someone else's password or other authentication credentials;

b) disclosing a personal password or other authentication credentials;

c) permitting another User to access or use accounts;

d) propagating computer viruses, worms, Trojan Horses, malware or any other malicious code;

e) preventing others from accessing an authorized service;

f) degrading or attempting to degrade performance or deny service; or

g) corrupting, altering, destroying, or misusing data or information.

12.3. Unlawful Use. Violations of Section 9.1.c) include, but are not limited to, using or attempting to use IT Resources to:

a) pirate software;

b) download, install, use, stream, or distribute unlawfully or illegally obtained media (e.g., software, music, movies);

c) override, remove or pause any security software installed on IT Resources by the University or at its direction;

d) commit criminal harassment, hate crimes, or libel and defamation;

e) commit theft or fraud; or

f) violate child pornography criminal laws.

12.4. Breach of University policies. Violations of Section 9.1.d) include, but are not limited to, using or attempting to use IT Resources to:

a) engage in academic dishonesty or plagiarism;

b) engage in discrimination and harassment, including making threats, stalking, or distributing malicious material; or

c) direct others to breach any provision of this policy.

12.5. Breach of Privacy. Violations of Section 9.1.e) include, but are not limited to:

a) accessing, attempting to access, or copying another person's ESI without authorization; or

b) divulging sensitive personal data to which certain University Members have access concerning faculty, staff, or Students without a valid and lawful administrative or academic reason.

13. Limitations on Personal Use by Employees

13.1. Employees are permitted to use IT Resources for occasional and limited personal use and consistently with this Policy and the Personal use of University Resources Policy.

13.2. The viewing or distribution of obscene, harassing, defamatory, discriminatory, pornographic or hateful material and messages by Employees using IT Resources is prohibited, unless such prohibition infringes upon academic freedom.

14. Investigation

14.1. Reports of conduct by Employees in contravention of this Policy will be addressed by the following means:

a) Harassment, violence or discrimination will be investigated under the Policy Against Harassment, Violence and Discrimination in the Workplace, and in accordance with any applicable collective agreements.

b) Other violations can be addressed by the procedures for receiving and resolving reports in section 10.3.

14.2. Reports of conduct constituting Sexual Violence by or against a student will be subject to investigation and sanctions under the Student Sexual Violence Policy.

14.3. Reports of conduct by Students in contravention of this Policy will be subject to investigation and sanctions under the Student Conduct Policy or Academic Integrity Policy, as applicable.

14.4. Reports of conduct constituting Harassment or discrimination not subject to another policy will be investigated under the Harassment and Discrimination Policy.

14.5. Reports of conduct by University Members other than Employees or Students in contravention of this Policy can be addressed by the procedures for receiving and resolving reports in section 10.3.

15. Consequences

15.1. Users who violate this Policy or any other University policy may be subject to disciplinary action in accordance with a collective agreement, if applicable, up to and including, but not limited to:

a) suspension of access to some or all IT Resources;

b) student expulsion from the University;

c) discipline and termination of employment; and/or

d) legal action.

16. Privacy

16.1. The University respects University Members' reasonable privacy expectations but University Members will not have an expectation of complete privacy when using the University's IT Resources.

16.2. University Members' privacy rights may be superseded by the University's right to protect:

a) the integrity of its IT Resources;

b) the rights of other University Members or Guests; or

c) the University's property.

16.3. The University reserves the right to monitor and log usage of its IT Resources.

16.4. The University also reserves the right to examine and preserve material stored on or transmitted through its IT Resources at its sole discretion. Examples of situations where the University may exercise this right include but are not limited to:

a) this Policy has been violated;

b) any other University policy has been violated;

c) any federal or provincial law has been violated; or

d) examination is necessary to protect the integrity of its resources.

16.5. The University will not normally access a University Member's ESI without consent except for certain limited and specific circumstances, including but not limited to:

a) investigations regarding security, illegal activity, or activity that may contravene the University's Policies and Procedures;

b) compassionate circumstances, as permitted by law;

c) where necessary to carry out urgent operational requirements during an employee's absence when alternative arrangements have not been made; and

d) compliance with law or legal obligations.

Note: The University will exercise these access rights only if administrative approvals have been granted by the Chief Privacy Officer.

16.6. Authorized University Employees or service providers under contract with the University, who operate and support IT Resources, may access ESI without notice to University Members in order:

a) to address emergency problems;

b) to perform routine system maintenance; or

c) for any other purpose required to maintain the integrity, security and availability of the IT Resources.

16.7. In the process of monitoring IT Resources, the University will:

a) use all reasonable efforts to limit access to University Members' ESI; and

b) not disclose or otherwise use any University Members' ESI that has been accessed, except in accordance with the applicable University policies, procedures and guidelines, and as permitted or required by law.

16.8. If the University is required to disclose a University Member's ESI, in accordance with the law, such disclosure will be reviewed and approved by the Chief Privacy Officer, prior to the release of the ESI.

17. Information Assets

17.1. Employees who have deleted files from one IT Resource, such as a computer hard drive are responsible for managing copies that may continue to exist in or on other IT Resources, such as shared drives. Employees are responsible for ensuring file management and disposition of Information Assets in accordance with the Records Management Policy, Records Classification and Retention Schedule, and Records Disposition Procedures.

17.2. Information Assets created or received outside of IT Resources, such as on a personal smartphone or computer must be stored on approved IT Resources as soon as possible to ensure continuity during an Employee's absence.

MONITORING AND REVIEW

18. This Policy will be reviewed as necessary and at least every three years. The Executive Director, Information Technology Services, or successor thereof, is responsible to monitor and review this Policy.

RELEVANT LEGISLATION

19. *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31

20. *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23

21. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5

RELATED POLICIES, PROCEDURES & DOCUMENTS

22. Information Security Policy

Records Management Policy

Records Retention and Classification Schedule

Records Disposition Procedures

Access to Information and the Protection of Privacy Policy

Personal Use of University Resources Policy

Student Conduct Policy

Academic Integrity Policy

Policy Against Violence, Harassment and Discrimination in the Workplace

Harassment and Discrimination Policy

Student Sexual Violence Policy

Technology Use Policy

Classification number	LCG 1109
Framework category	Legal, Compliance and Governance
Approving authority	Board of Governors
Policy owner	Vice-President, Academic and Provost
Approval date	May 2012
Review date	To be assigned
Supersedes	UOIT Policy on Acceptable Use of Information Technology, March 2006

Purpose

1. UOIT owns, maintains and manages computing and network resources to support the educational, instructional, research and administrative activities of the university. While individuals are free to use these valuable resources in pursuit of their individual and collective academic and administrative goals, it is equally important that safeguards are in place to ensure that the information, equipment and networks remain reliable, robust and secure on an ongoing basis. To that end, this policy is designed to guide in the management and use of the computing and network resources in a manner that is consistent with UOIT's values of integrity and responsibility, honesty and accountability, and intellectual rigour.

Policy

2. All members of the UOIT community, including employees, students, alumni and authorized guests, may be granted access to technology resources for use in their academic- and administrative-related activities. Users are expected to respect the university's good name in all electronic dealings with those outside the university and are responsible for familiarizing themselves and abiding by the university policies and regulations regarding the appropriate use of its technology resources. This includes, but is not limited to:

    - Respecting the rights of other members of the university community who study, work and live within it and refraining from transmitting or displaying on their devices images, sounds or messages that might create an atmosphere of discomfort, harassment or offense to others;
    - Refraining from conduct that may interfere with, access, or impair the activities of others;
    - Maintaining the integrity of their own IT account, taking reasonable measures to protect passwords and not sharing them with others;

- Using appropriate safeguards to secure technology resources against theft, damage or unauthorized access;
- Respecting the intellectual property rights of others, and using technology resources in a manner that is consistent with UOIT's contractual obligations to suppliers of intellectual property; and
- Abiding by university regulations, policies and by-laws and by federal, provincial and municipal laws.

While the university strives to maintain the privacy of information stored on UOIT technology resources, its confidentiality cannot be guaranteed. Additionally, in the performance of their duties, IT staff may access user files.

UOIT technology resources cannot be used for the purposes of non-university related advertising, mass emailing, political activities or to operate a business or other commercial enterprise without the written approval of the provost or vice-president, External Relations and the IT executive director.

UOIT considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information resident on university systems related to alleged inappropriate use, and to protect its network from systems and events that threaten to degrade operations.

Scope and authority

3. This policy applies to all members of the UOIT community, including employees, students, governors, alumni, guests, and other individuals who have been granted permission by virtue of their role and responsibilities, to access certain data, applications or systems that are part of UOIT's technology resources. The technology resources encompass all computing and networking resources owned by UOIT and those other resources that have been authorized by Information Technology Services to be connected to university facilities, including hardware, software, computer systems, applications, servers, databases, Internet, electronic communication, wire and wireless networks, campus telephone and voicemail systems available on and off campus.

   The Provost and Vice-President, Academic is responsible for the interpretation and administrative direction of this policy and associated procedures and guidelines to ensure their consistency with other university policies, as well as broader regulatory requirements.

Procedures

4. Incidents of inappropriate use of technology resources shall be investigated and dealt with by the university and will be subject to discipline and sanctions as are appropriate in the circumstances, including restrictions on or suspension of privileges or, for more serious cases, expulsion or termination from the university. Such matters will be dealt with in accordance with the Student Conduct Policy in the case of students, and with applicable collective agreements and policies for employees and volunteers. Offenders may also be prosecuted under federal, provincial and municipal laws, regulations and by-laws.

Review and Renewal

5. This policy and its associated shall be reviewed on a regular basis and at minimum every three years.