BOUCHER INSTITUTE
POLICY

Policy Title: Acceptable Use of Information Technology Policy
Date of Initial Board Approval: April 15, 2019
Date of Last Approved Revision:
Person(s) Responsible for Implementation & Adherence: Chief Financial Officer and IT Manager
Related Procedures:

I. Purpose

1. This Policy sets out the appropriate and responsible use of Information Technology (IT) Resources. The University provides IT Resources to Users in order to further the University's mission, including facilitating academic and administrative work through collaboration, discourse, and efficiency.
2. IT Resources are the property of the University and are intended to be used in a manner that is consistent with the University's mission and values. All Users are responsible for the manner in which they use IT Resources.
3. Before the University provides access to IT Resources, Users must:
    a. review this Policy
    b. acknowledge acceptance of the University's terms and conditions of use.

II. Scope and Application

This Policy applies to all Users of IT Resources and all IT Resources. The use of personally-owned equipment that involves the use of IT Resources is covered by this Policy.

III. Definitions

1. **"Electronically-Stored Information"** ("**ESI**") means Users' electronic information that is created and communicated in digital form and which is accessible through IT Resources.
2. **"IT Resources"** are made available to Users by the University, and may be hosted by the University or third parties, and include but are not limited to:
    a. 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;
    b. servers;
    c. databases;
    d. business systems;
    e. student and learning management systems;

f. websites;

g. computers and computer systems, laptops, workstations, computer labs, thin clients, mobile devices, storage devices; and

h. online collaborative tools including email, and social media sites (e.g. Ryerson Twitter, Facebook and YouTube sites).

3. **"Users"** means anyone who attempts to use or uses IT Resources. This includes, but is not limited to:

a. instructors (including professors, visiting professors, and scholars);
b. researchers;
c. staff;
d. students;
e. guests;
f. volunteers;
g. vendors, suppliers, and contractors.

IV. Policy

Authorized Use

1. Users shall comply with the following rules of acceptable use:

a. Use only those IT Resources for which the University has given you authorization, for its intended purpose(s).

b. Protect the confidentiality, integrity, and availability of IT Resources.

c. Abide by applicable laws and regulations.

d. Abide by University policies.

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

2. Users who fail to comply with the above rules of acceptable use may commit one or more of the violations indicated in Section 4.c and may be subject to disciplinary action.

3. The University reserves the right to limit or restrict the use of IT Resources based on:

a. institutional priorities;

b. financial considerations;

c. violation of this Policy or other University policies;

d. contractual agreements; or

e. provincial or federal laws.

Reporting

1. Users are responsible for guarding against misuse or abuse of IT Resources.
2. Users must promptly report any known or suspected misuse of IT Resources or violation of this Policy.
3. Reports should be directed to the unit, department, school, or administrative area responsible for the particular system or policy.

Violations

1. Unauthorized Use. Violations of Section 4.a.i.1 include, but are not limited to:
    a. using resources without specific authorization;
    b. using another User's electronic identity;
    c. accessing files, data or processes without authorization;
    d. using IT Resources to hide the User's actual identity;
    e. using IT Resources to interfere with other systems or Users;
    f. using IT Resources to deceive, harass or stalk another individual;
    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.
2. Breach of Confidentiality, Integrity and Availability of IT Resources. Violations of Section 4.a.i.2 include, but are not limited to:
    a. obtaining or using someone else's password or other authentication credentials;
    b. disclosing your password or other authentication credentials;
    c. permitting another User to access or use your 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.
3. Unlawful Use. Violations of Section 4.a.i.3 include, but are not limited to:
    a. pirating software;
    b. downloading, using or distributing illegally obtained media (e.g., software, music, movies);

c. committing criminal harassment, hate crimes, or libel and defamation;

d. committing theft or fraud; or

e. possessing or distributing child pornography.

4. Breach of University policies. Violations of Section 4.a.i.4 include, but are not limited to:

    a. engaging in academic dishonesty or plagiarism; or

    b. engaging in discrimination and harassment, including making threats, stalking, or distributing malicious material.

5. Breach of Privacy. Violations of Section 4.a.i.5 include, but are not limited to:

    a. accessing, attempting to access, or copying another Users' ESI without authorization; or

    b. divulging sensitive personal data to which Users have access concerning faculty, staff, or students without a valid administrative or academic reason.

Consequences

1. Users who violate this Policy or any other University policy may be subject to University disciplinary action, 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. termination of employment; and/or

    d. legal action as may be appropriate under existing University policies, employment contracts or collective agreements.

Privacy

1. The University respects Users' reasonable privacy expectations for ESI on its servers and networks. However, Users shall not have an expectation of complete privacy when using the University's IT Resources.
2. ESI may have an existence that differs from paper files. While paper documents may be shredded, ESI may exist in multiple locations, including multiple servers, disk drives, email attachments, and/or backup tapes or disks.
3. Users 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. Users are responsible for ensuring file management of ESI in accordance with the Records Management Policy and Retention Schedule.
4. Users' privacy rights may be superseded by the University's right to protect:

a. the integrity of its IT Resources;

b. the rights of other Users; or

c. the University's property.

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

6. The University also reserves the right to examine and preserve material stored on or transmitted through its IT Resources at its sole discretion. Examples may include if the University believes that:

    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.

7. The University will not normally access a User's ESI without the User's consent except for certain limited and specific circumstances. However, the University reserves the right to access a User's ESI without the User's prior consent in justifiable circumstances, including, but not limited to:

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

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

    c. compliance with law

    d. **Note:** The University will exercise this right only if appropriate administrative approvals have been granted.

8. University employees who operate and support IT Resources may access ESI without notice to Users in order:

    a. to address emergency problems;

    b. to perform routine system maintenance; or

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

9. In the process of monitoring IT Resources, the University shall:

    a. use best efforts to limit access to Users' ESI to the least invasive degree in general and;

b. use best efforts to limit access to Users' ESI to the least invasive degree of inspection required to perform its duties to maintain the IT Resources in circumstances where access to Users' ESI is unavoidable;

c. not seek out transactional information or the contents of ESI other than in accordance with this Policy; and

d. not disclose or otherwise use any Users' ESI that has been observed.

10. If the University is required to disclose a User's ESI, in accordance with the law, such disclosure shall be reviewed and approved by the Office of General Counsel and Board Secretariat, prior to the release of the ESI.