USE OF INFORMATION TECHNOLOGY POLICY

Approving Authority: President and Chief Executive Officer
Administrative Responsibility: Director, Policy Research and Advocacy
Original Approval Date: November 29, 2019
Date of Most Recent Review/Revision:
Related Policies, Procedures, and Documents: Student Executive Digital File Storage Procedures; Staff Digital File Storage Procedures; Wilfrid Laurier University Use of Information Technology (9.1).

---

1. Purpose

1.1. This policy establishes guidelines and expectations for the use of all Students' Union information technology.

2. Definitions

2.1. **Information technology**: Includes, but is not limited to:
- 2.1.1.1. Telephones;
- 2.1.1.2. Printers, copiers, and facsimile machines;
- 2.1.1.3. Computing or communication devices and associated peripherals;
- 2.1.1.4. Video and other multimedia devices;
- 2.1.1.5. Wearable devices;
- 2.1.1.6. Programs or software, including desktop applications, mobile apps, websites, and online or cloud-computing services;
- 2.1.1.7. Services and accounts, including email, network storage, and voicemail.

2.2. **User**: Any Students' Union volunteer or staff member provided access to information technology.
2.3. **Device:** A physical piece of information technology.

3. Jurisdiction/Scope

3.1. This policy applies to all Students' Union staff and volunteers.

4. Policy

4.1. The use of Students' Union information technology is ultimately subject to applicable provincial and federal law, Wilfrid Laurier University policies, and the terms of applicable

contracts and licenses.

4.2. The Students' Union makes information technology available to staff and volunteers to support the execution of their responsibilities;

4.3. Data Ownership:

4.3.1. All intellectual property created while in the employ of, or while using the devices provided by the Students' Union, shall be considered the property of the Students' Union;

4.3.2. Any creation of material on Students' Union property shall be considered the property of the Students' Union unless otherwise authorized by the President and Chief Executive Officer.

4.4. The Students' Union has the right and ability to access its information technology for the purposes of:

4.4.1. Technical maintenance, repair, and administration;

4.4.2. Ensuring the continuity of work;

4.4.3. Prevent or investigate misconduct.

4.5. Users of information technology must respect the privacy of others and not:

4.5.1. Disclose passwords, access codes, or other confidential authorizations;

4.5.2. Gain access to the accounts or files of other users;

4.5.2.1. Impersonate other users;

4.5.3. Distribute confidential internal records or documentations.

4.6. Users of information technology must refrain from:

4.6.1. Willfully introducing or distributing computer viruses, malware, phishing schemes, or other cyberattacks;

4.6.2. Restricting access to other legitimate users;

4.6.3. Allowing unrestricted and unaccompanied access to their devices;

4.6.4. Accessing, downloading, or distributing any material that contravene any applicable regulation or legislation;

4.6.5. The irresponsible and inappropriate use of email, included but not limited to:

4.6.5.1. Forwarding confidential emails to third parties;

4.6.5.2. Sending material that is fraudulent, defamatory, or of a harassing or threatening nature;

4.6.5.3. Misrepresentation.

4.6.6. Any activity that may constitute harassment or discrimination;

4.7. Users with an assigned email address (e.g. supresident@wlu.ca) must conduct all Students' Union business through that account;

4.7.1. Student executives should limit the use of their wlu.ca email address to Students' Union business and avoid personal communications;

4.8. Users must ensure that they enable any relevant security measures to limit third party access to their information technology.

4.9. Users of Students' Union information technology must adhere to the *Student Executive Digital File Storage Procedures* or the *Staff Digital File Storage Procedures*.

4.10. Users of Students' Union information technology must transition any relevant usernames

and passwords to their successors, including third-party tools or resources necessary to the role.

4.11. Users are permitted to use their personal mobile devices