IT 2001 Information Technology Acceptable Use

Classification:	Information Technology
Responsible Authority:	Director, IT Services
Executive Sponsor:	Vice President, Finance & Administration
Approval Authority:	President
Date First Approved:	2022-08-19 (date of original policy)
Date Last Reviewed:	N/A
Mandatory Review Date:	2024-06-30

PURPOSE

The Information Technology (IT) Acceptable Use Policy establishes specific requirements for the use of all IT resources at the University. The policy is intended to inform the University community of their rights and obligations when using University technology resources. It will provide users guidance on operating in a responsible, ethical & legal manner while respecting the rights of other users, the integrity of the IT facilities and pertinent license and contractual agreements.

SCOPE

This policy applies to all users of IT resources owned or managed by the University, including those purchased with research funds or external grants. Individuals covered by the policy include (but are not limited to) University employees, students, alumni, guests or agents of the administration, external individuals and organizations accessing university IT resources.

IT resources include all University owned, licensed, or managed hardware and software and use of the University network via a physical or wireless connection, regardless of the ownership of the device connected to the network. Hardware covered by this policy includes but is not limited to desktop computers, laptop computers, servers, mobile phones, tablets, and printers.

These policies apply to any technology administered in individual departments, the resources administered by central administrative departments, personally owned devices connected by wire or wireless to the campus network, as well as off-campus devices that connect remotely to the University's cloud-based or on-campus technology services.

Should there be a conflict between this document and a Collective Agreement between the University and one of its employee groups the applicable Collective Agreement will govern.

POLICY

Acceptable Use Policy

1.0 Purpose

Information Technology Services at St. Francis Xavier University supports the teaching, research, and administrative activities of the University. As a user of these IT resources, you may, depending on your role, have access to vital University systems, as well as sensitive data. Access to these resources, as well as internal and external networks, must be conducted in a responsible, ethical, and legal manner.

2.0 Your Rights and Responsibilities

As a member of the University community, you are provided with the work-related tools, computer systems, servers, software, databases, the campus telephone and voice mail systems and Internet access required for your role.

You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the University that apply to appropriate use of the University's IT resources and for exercising good judgment in their use. Just because an action is technically possible does not mean that it is appropriate to perform that action.

3.0 Acceptable Use

In general, acceptable use means respecting the rights of other users, the integrity of the physical facilities and all pertinent license and contractual agreements.

- You must use only the devices, accounts, and files for which you have authorization.
- You must not use another individual's account or attempt to capture or guess other users' passwords.
- You are responsible and accountable to the University for appropriate use of all resources assigned to you, including the devices, network connection, software and hardware. As an authorized user of IT resources, you must not provide unauthorized users access to the network using a University device that is connected to the University network.
- The University is bound by its contractual and license agreements respecting third-party resources. You are required to comply with all restrictions placed on these resources by IT Services.

- You must make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing the University's network and computing resources.
- You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- You must not use University IT resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other system users, or damage or degrade the performance of software or hardware components of a system.
- IT Services, and other University departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The campus network, servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the University community is explicitly forbidden.
- The University may choose to set limits on an individual's use of a resource through quotas, bandwidth limits, and other mechanisms to ensure that these resources can be used by anyone who needs them. Please review the Fair Share of Resources section of the "Acceptable Use Examples" for further clarification.
- It is recognized that limited, incidental personal use of University IT resources is acceptable as long as it does not interfere with job duties or other university responsibilities, does not consume an excessive amount of resources and does not put the University at risk or violate any other university policies. Specific departments may impose additional limits on computer use for non-work purposes in accordance with normal supervisory procedures as required.

3.1 Adherence with Federal, Provincial, and Local Laws

As a user of StFX’s IT resources you must:

- Abide by all applicable federal, provincial, and local laws.
- Abide by all applicable copyright laws and licenses. StFX University has entered into legal agreements or contracts for many of our software, subscribed content, and network resources, which require each individual using them to comply with those agreements. Compliance requirements will be clearly communicated to users.
- Observe copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information.

- Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work.

Please visit StFX University's Campus Copyright Guide for full discussion of your legal obligations relating to copyright

3.2 Other Inappropriate Activities

Use of IT resources for those activities that are not consistent with the educational, research and public service mission of the University and with the spirit of respect outlined in the University Community Code is prohibited. Prohibited activities include but are not limited to:

- Use of computing services and facilities for political purposes in a manner that promotes you as a candidate, results in or suggests the University itself is participating in a campaign, fundraising activity, or intending to influence legislation.
- Use of computing services and facilities for personal economic gain except as provided for in collective agreements and/or individual employment contracts.
- Unauthorized access to computing resources.
- Use of the services in a malicious, threatening, or obscene manner.

Links to Standards of Conduct policy and Community Code of Conduct:

Standards of Conduct Policy
Community Code of Conduct

3.3 Privacy and Personal Rights

- All users of the University's network and computing resources are expected to respect the privacy and personal rights of others.
- Unauthorized access to the account, email, data, programs, or files of another user is prohibited.

While the University does not generally monitor or limit content of information stored and/or transmitted on the campus network, it reserves the right to access and review such information under certain conditions including, but not limited to:

- Ensuring the integrity of IT resources and protection of University property;
- Investigating performance deviations and system problems (with reasonable cause);
- Conducting investigations regarding security, illegal activity, or activities that may contravene this policy, any other University policy, or any federal or provincial law;
- Carrying out urgent operational requirements during an employee’s absence where alternative arrangements have not been made;
- As may be necessary, ensuring that the University is not subject to claims of institutional misconduct; and
- Compliance with the law.

Access to user data on University IT resources will only be approved by specific personnel when there is a valid reason to access those files. Access by external law enforcement agencies is limited to situations where there is a valid subpoena and other legally binding request. Approval for all such access must come from the Academic Vice-President and Provost (for students and faculty) or the Vice-President, Finance and Administration (for staff). Information obtained in this manner may be admissible in legal proceedings or in an internal University administrative hearing.

3.4 User Compliance

When you use University IT resources (including University issued computing accounts), you agree to comply with this and all other computing related policies. You have the responsibility to keep up to date on changes in the computing environment, as published, using University electronic and print publication mechanisms, and to adapt to those changes as necessary.

4.0 Enforcement

If an employee is found to be in violation of the Acceptable Use Policy, the University may take disciplinary action up to and including termination from employment pursuant to the applicable Collective Agreement or individual employment contract. Users may also be subject to the restriction and possible loss of network privileges.

If a student is found to be in violation of the Acceptable Use Policy, the University may take action pursuant to the University's Conduct Code and/or legal action as appropriate. Such actions may include consequences up to and including suspension or expulsion from the University.

5.0 Related Links

Copyright and Fair Use
Copyright Infringement Policy

RELATED POLICIES

Policies which will support the 'IT Acceptable Use Policy':

Copyright Infringement Policy

IT XX: APPENDIX 1

Acceptable Use Examples

The following scenarios are intended to provide examples of acceptable and unacceptable uses of StFX's computing resources, based on the Acceptable Use Policy. These examples are not comprehensive but are merely illustrations of some types of acceptable and unacceptable use.

Authorized Use

Acceptable:

- While using someone else's computer from off campus, you connect to StFX to check your email. When you have finished, you log out of your account, closing any browser windows you may have used, and making sure your email password was not saved on the computer.
- While traveling, you ask a staff person to check your email for you by forwarding your email to their account, removing the forwarding on your return.

Unacceptable:

- While someone else is using a computer, you want to check your email. You ask them to log in, giving them your password to type in for you.
- While traveling on vacation, you ask a staff person to check your email for you by giving them your password.
- A colleague is out sick, and he/she was receiving responses for an event. The event is time-sensitive, so you attempt to gain access to their account by guessing their password.
- After having your computer hacked, you decide to download and run hacking tools yourself to help your friends out by checking for vulnerabilities on their computers.

Fair Share of Resources

Acceptable:

- You conduct a video conference with colleagues at another institution using your computer.
- You use a shared computer in a Library, computer lab, or departmental lab that you are authorized to use.

Unacceptable:

- You use your computer connected camera to display what is happening in your room 24 hours a day, 7 days a week on the Internet and list the site on major search engines and post it on listservs without prior authorization.
- While using a computer in a departmental lab, you alter its setup, so that each time it starts up, your favorite programs are started automatically.
- As an employee, you store substantial quantities of your photos, music, movies or software created and/or licensed solely for personal use on University resources (either on your workstation or a University server).
- You create or utilize an automated solution to register for courses in Banner, giving you not only an unfair advantage over other students, but also increasing the possibility of system degradation or failure.

Adherence to Laws

Acceptable:

- Storing legitimately obtained audio files for use in language instruction.
- Displaying a legally acquired copy (with copyright notice) of a video work on StFX premises to a group consisting primarily of students and faculty for educational purposes.

Unacceptable:

- Taking music you own, storing it on your computer, and setting up sharing to allow others to access those songs.
- Playing a video in front of an audience on StFX premises for entertainment purposes or for purposes that are not explicitly permitted by the content owner.
- You send out unauthorized and unsolicited email messages to other StFX community members in violation of Canadian Anti-Spam Legislation.

Other Inappropriate Activities

- Using a computer connected to StFX's campus network, you establish a commercial business, selling products or services over the Internet.
- You download, store, print and/or display materials that could be perceived by others as contributing to an intimidating, hostile, or sexually offensive working environment.

Privacy and Personal Rights

Acceptable:

- As part of an investigation into an employee's potential misuse of the campus network for copyright violations, permission is granted from an appropriate senior administrator for a supervisor to log into that employee's computer and check files that are stored on it.

Unacceptable:

- While checking the email system for possible problems, a systems staff person has to open a mailbox owned by someone else. In doing so, he or she reads the subject lines, finds one that looks interesting, and opens the email message.

User Compliance

Acceptable:

- When running licensed software at StFX, and finding a policy presented on the screen, an individual reads it and agrees to it before proceeding to the next screen.
- As malware alerts and other news are sent from IT Services, an individual takes appropriate action to protect his or her computers from those threats.

Unacceptable:

- When running licensed software at StFX, and finding a policy presented on the screen, an individual quickly clicks on the "I Agree" button without reading the policy or acknowledging responsibility for following it.

- As malware alerts and other news are sent from IT Services, an individual sets up an email filter to send the information directly to the trash.