Information Technology Acceptable Use Policy

Category:	Information Technology
Number:	IT1
Responsibility:	Director of Information Technology
Approval:	Administration, December 2015
Amendments:	Every three years or as circumstances warrant

PURPOSE

Services provided by the Information Technology Services department at Algoma University are intended primarily to serve the educational, research, and administrative purposes of the university. The university encourages the use of electronic communications for research, sharing information and knowledge in support of the university's mission and to conduct the university's business.

In particular, this policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and performance of IT Systems;
- To ensure that use of IT Systems is consistent with the principles and values that govern use of other University facilities and services;
- To ensure that IT Systems are used for their intended purposes; and
- To establish processes for addressing policy violations.

An electronic link or printed copy of this policy shall be given to the user at the time access to computing and communications facilities is given. An electronic link to the policy shall be displayed whenever possible on system logon screens.

SCOPE

This policy applies to all users of IT Systems, including but not limited to, students, faculty, university clubs, associations, staff, and general public connected to or communicating with University IT Systems. IT Systems include campus servers, networks, and facilities administered by the Information Technology Services department, as well as those administered by other departments and other University-based entities.

Access to university IT Systems is a privilege accorded at the discretion of the university. The use of IT Systems, even when carried out on a privately owned device that is not managed or maintained by Algoma University, is also governed by this policy.

Usage is also governed by all applicable University policies, by all applicable Federal, Provincial, and local laws and statutes, such as the Criminal Code of Canada, the Copyright Act, the Ontario Freedom of Information and Protection of Privacy Act, and the Personal Information Protection and Electronics Document Act, and by licenses governing the use of computer programs and documents of all kinds.

POLICY

IT Systems may only be used for their authorized purposes -- that is, to support the research, education, administrative, and other functions of Algoma University. The following categories of use are inappropriate and prohibited:

1. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not interfere, or attempt to interfere, with service to other users. This includes, but is not limited to, resource hogging, misusing mailing lists, propagating chain letters, virus hoaxes, or spam. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2. Harassing or threatening use. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another. This also includes sexual harassment, racial and ethnic harassment, gender harassment as well as any other harassment that an individual may find offensive in accordance with the Workplace Violence and Harassment Prevention Policy.

3. Use damaging the integrity of University or other IT Systems. This category includes, but is not limited to, the following activities:

> a. Attempts to defeat system security. Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking" or guessing and applying the identification or password of another user, compromising room locks or alarm systems, or disabling virus protection. This provision does not, however, prohibit IT System Administrators from using security programs within the scope of their job duties.
>
> b. Unauthorized access or use. The University recognizes the importance of preserving the privacy of users and data stored in campus IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non-Algoma University organization or individual may not use non-public IT Systems without specific authorization. Similarly, users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Students in computer labs must produce Algoma University identification on demand.
>
> c. Unauthorized services and devices. Privately owned computers and other devices may not be used to host sites or services on the Algoma University network without specific authorization. Network devices including, but not limited to, repeaters, switches, routers, and wireless access points, require authorization prior to being connected to the university network.
>
> d. Interception. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by network monitoring, running network sniffers, or otherwise tapping phone or network lines.
>
> e. Disguised Use. Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.
>
> f. Distributing computer viruses. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

g. Modification or removal of data or equipment. Without specific authorization, users may not remove or modify any University owned equipment or data from IT Systems.

h. Download or use unlicensed or unauthorized copies of computer software or media. Users must not use the Algoma University network to illegally download or upload copyrighted material or licensed material. This includes 'torrenting' or downloading of any illegal videos, images, text, audio, and any other form of media.

4. Use in violation of law. Illegal use of IT Systems; that is, use in violation of civil or criminal law at the federal, provincial, or municipal levels is prohibited. Examples of such uses are: receiving, transmitting, or possessing child pornography; infringing copyrights; and making threats.

5. Personal Account Responsibility. Users are responsible for maintaining the security of their own passwords. Any password changes must follow published guidelines for passwords. Accounts and passwords are normally assigned to single users and must not be shared with any other person. Users are also not permitted to use their University computer account without authorization after an individual's relationship with the University has terminated;

6. Political Use. Use of IT Systems in a way that suggests University endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes University involvement.

7. Personal Use. Employees must not use IT Systems for personal use that interferes to any degree with the performance of their job responsibilities.

The above clauses are representative examples and do not comprise a comprehensive list of unacceptable uses. Any exception to the above clauses must have the prior approval of the appropriate University authority.

ABUSE OF POLICY

Abuse or misuse of IT Services may not only be a violation of University policies but also of the Criminal Code of Canada. In any alleged abuse or misuse, authorization can be requested from the Director of Information Technology to examine directories, files, or other electronic records that are relevant to the investigation of the allegation.

Allegations that a student is responsible for abuse will be investigated and dealt with under the Student Code of Conduct. Allegations that a staff member is responsible for abuse will be investigated by the Human Resources department.

If a User witnesses abuse of this policy, they are required to notify the Information Technology Services department by emailing abuse@algomau.ca.

AUTHORITY

Exceptions to this policy must have authorization from the Director of Information Technology Services.