Sheridan | Get Creative	THE SHERIDAN COLLEGE INSTITUTE OF TECHNOLOGY AND ADVANCED LEARNING	
TITLE: ACCEPTABLE USE POLICY		
Date of Approval: May 16, 2011; May 13, 2014; June 24, 2015 **Effective Date: June 24, 2015**	**Mandatory Review Date:** **3 year review**	**Approved By:** ☐ Board of Governors ☒ President's Council ☐ Senate

1. PURPOSE:

This Acceptable Use Policy (the "Policy") governs the use of computer networks, all computers and other devices connected to those networks, and the resources made available thereby at Sheridan. It applies to all employees, students, alumni and any other users of the information resources at Sheridan.

This policy exists in order for Sheridan to:

- Maintain and operate the information resources
- Ensure the proper use of the information resources
- Ensure compliance with the law
- Meet Sheridan's other operational needs

2. SCOPE:

All Sheridan employees, students, alumni and any other users of Sheridan's Information Resources are responsible for reading, understanding and complying with this Policy.

3. DEFINITIONS

a. "Commercial Electronic Message" means an electronic message that, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity.

b. "CASL" means Canada's Anti-Spam Legislation.

4. POLICY STATEMENT

4.1 Use of Information Resources

The access granted to Sheridan's information resources is intended for Sheridan business and education use and any incidental personal use should not be to the detriment of Sheridan or any of its students or employees. Therefore each Account holder or other user of Sheridan's resources must comply with the following:

Accounts:

- Accounts may only be accessed by the user to whom the account was assigned unless otherwise stated in this policy.
- The Account and password must be kept secure. Users must log out of the Account or lock access to a resource when leaving it unattended. The password should never be shared.

Account Use:

- In the case of employees, access must not be used for the purpose of carrying out a personal or private business enterprise and/or sending electronic messages to promote outside commercial activity without written authorization from Sheridan. In the case of all other users, access must not be used for the purpose of carrying out a business enterprise and/or sending electronic messages to promote outside commercial activity without written authorization from Sheridan.
- Users must not use Sheridan information resources for personal or political causes.

Legal / Compliance:

- Access is not to be used for any illegal purpose.
- Access must not be used by any person for the purpose of gaining illegitimate or unauthorized access to user accounts, resources, files, systems, databases, or information within any of Sheridan's systems or for the purpose of breaking into any other system outside Sheridan. No person shall change, enter, add, delete or alter in any way any information within Sheridan's systems, files and databases without proper authorization.
- Users must not use Sheridan information resources or access for the creation, transmission, storage, access or viewing of materials prohibited by federal and/or provincial law, or which, in the opinion of Sheridan, are offensive by community standards and values.
- Access must not be used to harass, threaten or annoy others or to store or send messages which are pornographic, obscene, abusive, threatening, libelous, defamatory or harassing. This would include sending unwanted e-mails to another after being requested not to do so. The User is responsible for ensuring the use of the Account conforms to all Sheridan policies and procedures including but not limited to the Student or Employee Code of Conduct and Harassment and Discrimination Policy.
- Users must be aware of and respect all copyrights, trademarks and other intellectual property rights for materials, including the use of Sheridan logo.
- Users must not represent themselves as acting on behalf of Sheridan unless properly authorized to do so.
- Users must not use Sheridan information resources for the creation, transmission, storage, access or viewing of materials, or any use of Sheridan's systems in a way that compromises Sheridan's legitimate interests.

Malicious Activity

- Users must not attempt to circumvent any security or control measures implemented on Sheridan systems.
- Users must not use any Sheridan computing facilities for the purpose of creation, development, storage, replication or transmittal of any program, code, subroutine or other means intended to disrupt, interfere, destroy or corrupt the normal operation of systems, data, or the work of others (i.e. viruses, worms, hack utilities).
- Access must not be used to monitor, interfere with or destroy work being done by others.
- Users must refrain from monopolizing systems; overloading networks with excessive data; degrading services; or wasting computer time, disk space, printer paper or other resources.

Privacy / Confidentiality / Integrity

- Sheridan operates in compliance with existing freedom of information and protection of privacy legislation. Users who access personal information of students, employees and others on behalf of Sheridan must keep such information confidential and use it only for meeting their responsibilities to Sheridan.
- Individuals must not access information about their colleagues, their relatives or their acquaintances under any circumstances, unless authorized.
- Individuals must not alter information about themselves, their colleagues, their relatives or their acquaintances under any circumstances, unless authorized.

Security

- Users must report instances of misuse or unauthorized activity to Information Technology immediately. Passwords must be changed immediately if an account is compromised or there is a strong suspicion that it has been compromised.
- Users must use security features (virus protection for example) provided by Sheridan, as required. If users suspect that their computer is infected by a virus, users must ensure that this is remediated.

Electronic Communications

- Employees sending a Commercial Electronic Message on behalf of Sheridan are required to comply with CASL, follow all applicable Sheridan procedures and must seek assistance if in doubt as to whether their messaging activity involves sending a Commercial Electronic Message.
- Users must not attempt to misrepresent the originator of any communication he or she initiates or forwards.
- All Sheridan electronic communications must utilize a platform approved by Sheridan. All employees will only use their Sheridan e-mail addresses for email correspondence. Sheridan e-mail addresses shall be considered the official means for communicating with all students, and employees and may in some cases be the

sole means of communication. Employees and students are required to check their email account(s) on a frequent and consistent basis in order to stay current with Sheridan-related communications unless on a Sheridan approved leave. Students are responsible for checking both their @sheridancollege.ca email account for Office of the Registrar and/or other Sheridan administrative communications and their @sheridan.desire2learn.com SLATE messaging system account for course-related communications. Employees and students have the responsibility to recognize that certain communications may be time-critical. Failure to receive and/or read a notification in a timely manner does not release the employee and/or student from the obligation to know of and/or comply with its content.

4.2 All guidelines and policies apply to all resources whether access is initiated on-site, through a remote location or using personal and/or individual equipment.

4.3 Users should obtain clarification from the Information Technology department when unsure about whether a planned use is acceptable.

4.4 Monitoring of Use

Sheridan recognizes the value of being able to work and study without concern of being under constant surveillance and therefore does not routinely monitor the activities of individuals. However, Sheridan does perform periodic random audits for system security purposes and will investigate situations based on reasonable suspicion of a breach. As such, users should have no expectation of privacy when using Sheridan's network. All telephone and computer systems at Sheridan (including hardware, software for which Sheridan is the licensee or owner, and storage space) remain the property of Sheridan and are provided to advance its vision and goals. Accordingly, Sheridan reserves the right to examine any electronic files including emails, and web-based personal emails accessed on Sheridan network, where Sheridan, in its sole discretion, determines that it has reason to do so.

The situations in which Sheridan may decide to examine a user's electronic files include but are not limited to:

- During an investigation of a suspected breach of existing laws, policies, or guidelines; or
- If compelled to do so by any law, including a request for information under the Freedom of Information & Protection of Privacy Act; or
- Where necessary to carry out urgent operational requirements during an employee's absence when alternative arrangements have not been made; or
- When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise protect the integrity of the information communication technology systems; or
- During period random audits for system security reasons

Access will only occur after appropriate authorization is received in accordance with Sheridan's IT Protocol.

It should be noted that files stored electronically have an existence that differs from paper files. While paper documents may be shredded, electronic documents may exist in multiple locations — on multiple servers or other backup and storage devices. The act of deletion from hardware does not assure permanent erasure. Users should be aware that

files stored on Sheridan's network may be accessed by Sheridan after the files are deleted.

4.5 Account Management

Individual managers have the responsibility of requesting either account deletion or removal of privileges when their employees permanently or temporarily leave and/or change positions. The changes will ordinarily be activated the day following the date of termination/reassignment. For accounts that are deleted from the system, data that is contained in all directories, whether work related or personal, will usually be deleted from the system 30 days after account access is suspended. Data in voice mailboxes will be cleared on the date of termination/reassignment, unless otherwise requested by the employee's manager or Human Resources. Information Technology also inactivates accounts based on employees termination/leave dates and student withdrawal/graduation dates. All deletion of information as contemplated by this section will be suspended when it is or could reasonably be expected to become relevant to a legal claim.

Accounts that belong to active employees who are going on leave from Sheridan for more than 60 days, and who will not require access while they are absent from Sheridan, should be disabled immediately to discourage unauthorized access.

I.T. should be contacted to discuss archiving or transferring data if required. Generally, temporary access to someone else's Account will not be granted by Information Technology.

4.6 Policy Violation

Sheridan may take appropriate disciplinary measures in cases of attempted violation of the provisions of this policy, regardless of the success or failure of the attempt.

Opportunities for review and discussion of the alleged violation will be subject to the "Non-Academic Appeal Procedure" for students, or in the case of employees, the provisions of Sheridan's employees groups' collective agreements and/or terms and conditions of employment.

Any attempt to circumvent local, provincial, federal or international laws through the use of Sheridan owned facilities may result in litigation against the offender by the appropriate authorities. Note: Some violations of this Policy are also covered under existing legislation, including but not limited to the Criminal Code of Canada and the Copyright Act or under other Sheridan policies such as the Harassment and Discrimination Policy.

Please note that any violation of this Policy by Sheridan employees may result in serious sanctions up to and including dismissal. Any violation by students may result in serious sanctions up to and including expulsion. If there are any questions concerning the Policy, please direct those inquiries to one of the following:

- Human Resources
- Student Services
- Information Technology (I.T.) HelpDesk at extension 2150 or helpdesk@sheridanc.on.ca

Issues relating to students misuse will be referred to the Office of Student Rights and Responsibilities, Student Affairs; issues involving employees misuse will be referred to Human Resources.

4.7 Discontinuing Access

Access to Sheridan's IT systems including but not limited to e-mail, Internet access, departmental network service, learning management systems, telephone, fax and voice-mail, and other technologies can be terminated or suspended without notice to the user for proper cause, including when:

- The user has violated this policy or there is reasonable suspicion the user has violated this policy;
- Employment of the user is terminated regardless of reason;
- The user is on leave from Sheridan for greater than 60 days regardless of reason;
- There is account activity that overextends the resources or otherwise disrupts the functioning of the network;
- A user's account has been compromised or accessed by an unauthorized party.

This list is not exhaustive and does not represent all the circumstances where access to Sheridan's IT systems could be terminated or suspended.

4.8 Roles and Responsibilities

Managers

Managers are responsible for:

- Determining and arranging for their employees' specific system access;
- Informing their employees on the appropriate use of Sheridan's information resources;
- Reporting instances of suspected misuse or unacceptable use of Sheridan's information resources by a Sheridan employees, contractor, volunteer, co-op student, student worker, visitor or other person for whom they are responsible to Human Resources and system security concerns/vulnerabilities to Information Technology;
- Ensuring that systems access is removed when an individual leaves Sheridan or their responsibilities change.

Employees

Employees are responsible for reporting instances of suspected misuse or unacceptable use of Sheridan's information resources by a Sheridan student to the Office of Student Rights and Responsibilities, Student Affairs, and system security concerns/vulnerabilities to Information Technology.

Director, Information Security & Compliance

The Director, Information Security & Compliance is responsible for:

- developing and maintaining policies designed to protect information resources;
- establishing and maintaining high-level standards and related procedures for Sheridan's information and systems;
- Selecting, implementing and administering controls and procedures to manage information security risks;
- receiving reports of incidents and threats that may have an impact on Sheridan's information resources;
- ensuring that all reported security breaches are fully investigated and the appropriate remedial action is taken;
- acting as Sheridan's representative to external bodies on matters relating to IT security;
- providing information security advice to all levels of Sheridan community

Information Technology Employees

Information Technology Employees are responsible for protecting Sheridan's systems and networks.

Information Technology Steering Committee

The Information Technology Steering Committee is responsible for approving Sheridan platforms.

Human Resources

The Human Resources department is the primary contact for a manager dealing with issues relating to any Sheridan employees and the misuse of his/her rights and responsibilities. Human Resources will work with managers to take appropriate action in managing situations of misuse.

Student Affairs

Student Affairs is the primary contact for dealing with issues relating to students and the misuse of his/her rights and responsibilities. Student Affairs will initiate any formal disciplinary actions involving students. Problems or questions in this regard should be referred to the Office of Student Rights and Responsibilities, Student Affairs.

5. RELATED DOCUMENTS

- Password Change Procedure
- Acceptable Use Canada's Anti-Spam Legislation (CASL) Procedure for Sheridan Employees
- CASL Checklist
- CASL Explanatory Slide Deck
- CASL (Canada's Anti-Spam Legislation) Q & A
- Social Media Policy
- Employee Technology Policy
- Records and Information Management Policy