Sheridan	THE SHERIDAN COLLEGE INSTITUTE OF TECHNOLOGY AND ADVANCED LEARNING	
Title: Acceptable Use Policy		
Original Date: May 16, 2011 **Date of Approval:** November 13, 2024	**Effective Date:** November 13, 2024 **Last Review Date:** November 13, 2024	**Approved By:** ☐ Board of Governors ☒ President and Vice Presidents

1. Purpose

This Acceptable Use Policy ("Policy'') governs the utilization of technology systems and tools, including computers, software, communication networks, and cloud-based technologies at the Sheridan College Institute of Technology and Advanced Learning ("Sheridan''). The Policy does not attempt to anticipate every situation that may arise and is meant to serve as instructions for anyone accessing Sheridan Information Technology ("IT") Resources.

This policy exists for Sheridan to:

- Maintain and operate Sheridan IT Resources
- Ensure the proper use of Sheridan IT Resources
- Ensure compliance with the law
- Meet Sheridan's operational needs

2. Scope

This Policy applies to all Sheridan employees, students, alumni, contractors, and other individuals using Sheridan IT Resources. The requirements set out in this Policy are applicable to the use of all data, systems, electronic and computing devices, and services owned and/or managed by Sheridan.

3. Definitions

"**Access**" refers to access to systems, services, and information that is accessible through such services.

"**Account**" refers to an identity created for an individual in a computer or computing system, consisting of a unique username and password. This identity allows the individual to log in and Access Sheridan IT Resources.

"**Account Holder**" or "**Individual**" is the individual for whom the Account was provisioned, and the individual who uses or is responsible for the Account.

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

"**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.

"**Information Technology (IT)**" shall refer to Sheridan's Information Technology (IT) Department.

"**Information Technology (IT) Resources**" includes all Sheridan owned or managed hardware and software assets, including computers, communication networks, systems / applications, and cloud-based solutions.

4. Policy

Access granted to Sheridan IT Resources is intended for Sheridan business and educational use and any incidental use outside of Sheridan should not be to the detriment of Sheridan or any of its students or employees. IT Resources will not be used for employment purposes outside of Sheridan.

All requirements below apply regardless of whether Access is initiated on-site, through a remote location, or using personal and/or individual equipment.

4.1 Account Use

- Accounts may only be accessed by the Individual to whom the Account was assigned unless otherwise stated in this Policy.
- The Account and password must be kept secure. Individuals must log out of the Account or lock Access to an IT Resource when leaving it unattended. The password should never be shared.
- The Account Holder is fully responsible for any information or data, including those in digital storage services or other resources tied to their Account.
- Account Holders must not use Sheridan Accounts for personal or political reasons.
- Accounts must not be used for conducting personal or private business and/or sending electronic messages to promote outside commercial activity without written authorization from Sheridan.

4.2 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 Accounts, IT Resources, files, systems, databases, or information within any of Sheridan IT Resources or for the purpose of breaking into any other system outside Sheridan. No one shall view, change, enter, add, delete or alter any information within Sheridan IT Resources without proper authorization.
- Account Holders must not use Sheridan IT 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.
- Individuals are expected to communicate in a professional and respectful manner, adhering to all Sheridan policies and procedures including, but not limited to, the Student Code of Conduct, Code for Professionalism and Civility, and Harassment and Discrimination Policy.
- Access must not be used to harass, threaten, or annoy others or to store or send messages

which are obscene, abusive, threatening, libelous, defamatory, or harassing. This would include sending unwanted e-mails to another after being requested not to do so.
- Using IT Resources to visit pornographic sites, or for the storage or dissemination of pornographic material, is prohibited.
- Individuals must be aware of and respect all copyrights, trademarks, and other intellectual property rights for materials, including the use of the Sheridan logo.
- Individuals must not represent themselves as acting on behalf of Sheridan unless properly authorized to do so.
- Individuals must not use Sheridan IT Resources for the creation, transmission, storage, Access or viewing of materials, or any use of Sheridan IT Resources in a way that compromises Sheridan's legitimate interests.

4.3 Malicious / Inappropriate Activity

- Individuals must not attempt to circumvent any security or control measures implemented on Sheridan systems.
- Individuals must not use any Sheridan IT resources for the purpose of creation, development, storage, replication or transmittal of any program, code, subroutine, or other means (e.g., viruses, worms, hack utilities) intended to disrupt, interfere, destroy, or corrupt the normal operation of systems, data, or the work of others.
- Access must not be used to deliberately interfere with or destroy one's own work or the work of others. Authorized Sheridan representatives might at times monitor Accounts for security purposes based on reasonable suspicion of a breach. *For more details, see section on 'Monitoring of Use' below.*
- Individuals must refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, disk space, printer paper, or other resources.

4.4 Privacy / Confidentiality / Integrity

- Sheridan operates in compliance with existing freedom of information and protection of privacy legislation. Individuals 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.

4.5 Security

- Individuals must use password protection and security features (e.g., endpoint / device protection software for example) provided by Sheridan, as required.
- Individuals must not open message attachments or click on hyperlinks from unknown sources.
- Individuals must not send sensitive information from their devices or Accounts, that is not appropriately protected (e.g., encrypted or tagged as sensitive).
- If an Individual suspects that their Account has been compromised, they must reset their passwords immediately at the 'Sign in' prompt. They should also reach out to IT.

4.6 Removable Media (only applicable to employees)

- Information should only be stored on removable media when required in the employee's role (i.e., USB shared between two employees during a conference).
- Removable media must not be utilized to store and/or transmit confidential or restricted data unless absolutely necessary; if there arises such a requirement, the removable media should be encrypted as outlined in Sheridan's Encryption Standard.
- Any unknown removable media that is found unattended must be surrendered to security or the IT Service Desk and NOT inserted into any Sheridan issued device.
- Employees must take reasonable measures to secure removable media when not in use and prevent unauthorized Access.
- Upon completion of the assigned duties, all data must be deleted from the removable media.

4.7 Data Security

- All institutional data is owned by Sheridan and must be protected appropriately.
- Stewardship of Sheridan's data records should adhere to the Records and Information Management Policy.
- Individuals must not view, copy, alter, or destroy data, software, documentation, or data communications belonging to Sheridan or another Individual without authorized permission.
- Individuals must only access data provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent.
- Individuals must follow all company-sanctioned data removal procedures to permanently erase data from devices once its use is no longer required.

4.8 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 while they use Sheridan IT Resources. Sheridan does, however, perform periodic random audits for system security purposes and will investigate situations based on reasonable suspicion of a breach. All Sheridan IT Resources 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 a 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 an Individual's electronic files include but are not limited to:

- During an investigation of a suspected breach or violation 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 *Personal Health Information Protection 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 periodic random audits for system security reasons.

Access will only occur after appropriate authorization is received.

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

4.8.1. Electronic Discovery/Analysis

At certain times, Sheridan might need access to a device for security and/or electronic discovery/analysis purposes. In these situations, the Individual is responsible for providing the device to the IT Security department along with any necessary device codes (e.g., passwords, codes / device personal identification numbers) to obtain access. Access will be undertaken in a manner that, to the extent possible, preserves the privacy of the Individual.

4.9 Account Management

Managers have the responsibility of requesting either Account revocation or removal of privileges to Sheridan's IT Department when their employees:

- Permanently leave Sheridan; or
- Go on temporarily leave; or
- Change positions

The changes to account privileges will be activated, when possible, within 24 hours of the date of termination or reassignment.

Accounts that are suspended / locked when employees leave, are deleted within thirty days along with all data contained in the Individual's mailboxes, Microsoft OneDrive folders, Microsoft Teams communications / messages, unless other arrangements have been approved and confirmed.

Any 'shared / group / team' data such as SharePoint folders and files of which the Individual was a part of and any Teams channel (e.g., group – chat communications / messages) will not be deleted.

Data in voice mailboxes will be cleared on the date of termination/reassignment, unless otherwise requested by the employee's manager or Human Resources. Sheridan's IT department also deactivates Accounts based on an employee's termination/leave date and student withdrawal/graduation date. All deletion of information as contemplated by this section will be suspended when it is or could be expected to become relevant to a legal claim, audit, or investigation.

Accounts that belong to active employees who are going on leave from Sheridan for more than sixty days, and who will not require Access while they are absent from Sheridan, should be disabled immediately to discourage unauthorized Access. There may be exceptional circumstances where Access is required; this will be determined by the Individual's manager in consultation with their human resources business partner. Sheridan may access a former employee's emails, electronic files, or other electronic communications to obtain records necessary for business continuity or other legitimate business or legal reasons. Access will be undertaken in a manner that, to the extent possible, preserves the privacy of former employees. Access requests will be reviewed on a case-by-case basis and subject to approval as outlined in the guideline for departed employees' data.

4.10 Discontinuing Access

Access, all or in part, to Sheridan IT Resources can be terminated or suspended without notice to the Individual for proper cause, including when:

- An Individual has violated this Policy or there is reasonable suspicion they have violated this Policy; or
- Employment of the Individual is terminated regardless of reason; or
- The Individual is on leave from Sheridan for greater than sixty days regardless of reason; or
- There is Account activity that overextends the resources or otherwise disrupts the functioning of the network; or
- An Individual'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 IT Resources could be terminated or suspended.

5. 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. All Sheridan electronic communications must utilize a platform approved by Sheridan. All employees will only use their Sheridan e-mail addresses for all communications around Sheridan business and related activities.

- Sheridan e-mail addresses shall be considered the official means of communicating with all students and employees and may be the sole means of communication.
    - Account Holders should check their email account(s) frequently and consistently 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 the messaging system associated with the designated learning management system for course-related communications.
    - Individuals are responsible for recognizing that certain communications may be time critical. Failure to 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.

To maintain efficient and effective communication within our institution, all students, staff, and faculty are required to use the published support channels when contacting service areas for support. Direct communication with Individuals or escalating issues outside of these designated channels is discouraged, as it can lead to delays, miscommunication, and inefficiencies.

7. Roles and Responsibilities

7.1 Sheridan's Information Technology Department (IT)

Besides the items listed across this Policy, IT is responsible for:

- Providing secure and reliable IT infrastructure and monitoring systems for compliance.
- Implementing technical controls to safeguard data, managing access rights, and ensuring that all Sheridan IT Resources are protected against unauthorized access and misuse.
- Providing guidance on best practices, offers training on acceptable use standards, and regularly updates security protocols to adapt to emerging threats.

7.2 Managers

Managers are responsible for:

- Determining and arranging for their employees' specific Access;
- Ensuring their employees are familiar with policies around the appropriate use of Sheridan IT Resources;
- Reporting instances of suspected misuse or unacceptable use of Sheridan IT Resources by a Sheridan employee, 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 IT;
- Ensuring that Access is removed when an Individual leaves Sheridan or their responsibilities change.

7.3 Employees

Employees have a shared responsibility towards protecting Sheridan IT Resources. Employees are responsible for reporting instances of suspected misuse or unacceptable use of Sheridan IT Resources by a Sheridan student to the Office of Student Rights and Responsibilities, Student Services, and system security concerns/vulnerabilities to IT.

7.3 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.

7.4 Student Services

Student Services is the primary contact for dealing with issues relating to student conduct. Student Services will initiate any formal disciplinary actions involving students. Complaints regarding student violations related to this Policy should be referred to the Office of Student Rights and Responsibilities, Student Services.

8. Policy Compliance

Individuals should obtain clarification from their department and IT for any IT related questions (i.e., when unsure about whether a planned use of a software / tool is acceptable), using the below channels:

- Service Sheridan (or)
- Phone: 905-845-9430 ext. 2150 (or)
- Support Chat

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

Any attempt to circumvent local, provincial, federal, or international laws utilizing Sheridan IT Resources may result in litigation against the offender by the appropriate authorities.

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:

i. Human Resources
ii. Student Services
iii. IT using the channels listed above

Issues relating to student misuse will be referred to the Office of Student Rights and Responsibilities, Student Services; issues involving employee misuse will be referred to Human Resources.

The Responsible Office for this Policy is the AVP and CIO as delegated by the Vice President, Administrative Services.

9. Related Documents

CASL Checklist
CASL Explanatory Slide Deck
CASL (Canada's Anti-Spam Legislation) Q & A
Criminal Code of Canada
Copyright Act Canada
Discrimination and Harassment Policy & Procedure
Employee Technology Policy
Free Speech Policy
Social Media Policy
Records and Information Management Policy
Privacy Policy
Password Management Procedure
Guideline for Access to Departed Employees' Emails, Files or Communications
Sheridan's Encryption Standard
Information Security Policy