POLICY:	**Information Technology Acceptable Use & Security Policy**
APPROVED BY EXECUTIVE:	**July 9th, 2014**
SUPERSEDES POLICY:	**Information Technology Acceptable Use & Security Policy - January 18th, 2012**

PURPOSE: Sault College provides computing resources so students, employees and others can complete college-related tasks for college-related purposes. Use of these resources must be made in accordance with this policy and all applicable laws.

SCOPE: This policy applies to students, employees and others and applies to use of the College System.

PROCEDURE:

This policy is administered by the Chief Information Officer, Information Technology Services or his/her delegate.

This policy shall be posted in computer labs and periodically brought to users' attention. It will be shared at all new hire orientation sessions.

Definitions

"Employee" for the purposes of this policy includes independent contractors who are given access to the College System for the purpose of undertaking contractual duties to the College.

"College System" means IT services, network, facilities and equipment owned or operated by the College for the use of employees and others.

"Confidential Information" means information about the College's business that is not generally known to the public and includes student personal information or any other information that is regulated by the *Freedom of Information and Protection of Privacy Act*.

Rules for Acceptable Use

Users must comply with all laws, comply with all College policy, and comply with the following specific rules:

1. Access and Identity

   (a) Users must only use and access the College System as authorized and to the extent authorized by the College.

   (b) Users must use their own account to access the College System.

   (c) Users must not let anyone else use their identity to access the College System. Password sharing is prohibited.

   (d) Students using the College System from open access labs and other similar spaces must produce Sault College identification on demand.

(e) Any commercial electronic message (CEM) sent by a College employee to recipients in Canada, must comply with Canada's Anti-spam Legislation (CASL)

(i) This includes but is not limited to: emails and other electronic messages sent to students, prospective students, parents of students or prospective students, alumni, donors, governmental bodies, vendors and suppliers, members of the general public, and others.

(ii) Users of the College system with valid saultcollege.ca email addresses are in compliance with the CASL and are considered to have given 'implied' consent. Some relevant examples of implied consent include where the recipient is one or more of the following: (a) a student currently enrolled at the College; (b) a current member of the alumni association or someone who was a member of the alumni association within the past 2 years; (c) a person who made a donation to the College or volunteered for the College in the past 2 years; (d) a person who made an inquiry or application to the College in the past 6 months; or (e) a person who provided their email address to the College without prohibition on receiving CEMs, and the message relates to the recipient's job, title or official capacity.

2. Express Restrictions on Use

(a) Users must not use the College System to violate another person's intellectual property, including by using the College System to engage in the theft of software, music, movies or other material outlined by the Canadian Copyright Act.

(b) Users must not create, view, transmit, store or copy information that is pornographic, obscene, threatening, defamatory or harassing or that expresses or implies an intention to discriminate.

(c) Employees must not engage in personal use of the College System that interferes to any degree with the performance of their job responsibilities.

(d) Users must not use the College System for the purpose of carrying out a business enterprise without written authorization from the College.

(e) Users must not use the College system for personal or political causes.

(f) Users must not use the College System for a purpose or in a manner that is inconsistent with the College's legitimate interests.

3. System Security Duties

(a) Users must not purchase and/or install software on the College System without authorization from Information Technology Services.

(b) Users must not attempt to circumvent any security or control measures on the College System.

(c) Users must refrain from recording passwords in a place that they could be seen by others.

(d) Users must log out to protect their account from being accessed by others.

4. Employee Duty to Protect Confidential Information

Employees must take reasonable steps to ensure that Confidential Information stored on the College System is not lost or stolen or subject to unauthorized access, disclosure or copying, including by complying with the following rules, including by:

(a) Being present when printing Confidential Information

(b) Situating computer display terminals to prevent intended disclosure of Confidential Information

(c) Using secure passwords for accessing the system

(d) Refraining from recording passwords where they may be seen by others

(e) Portable hand held devices issued to users must have secure passwords and users must activate any GPS software that is made available by the College to assist in locating the device in cases of theft or lost property.

(f) Laptops issued to users must have secure passwords and users must activate any GPS software that is made available by the College to assist in locating the device in cases of theft or lost property.

(g) Student or confidential College information stored on any portable device (eg: memory sticks etc.) or laptops must be encrypted.

(h) Returning all equipment and portable storage media to Information Technology Services for secure disposal

5. Reporting Duties

Users must report the following to the Chief Information Officer or Human Resources

(a) Use of the College System that is illegal, that conflicts with this policy and that conflicts with other College policy

(b) Any suspected loss or theft and any unauthorized access, disclosure or copying of Confidential Information

Privacy

The College System is operated by the College so students, employees and others can complete college-related tasks for college-related purposes. The College has a strong interest in the information on its system and must have access to it for many legitimate reasons, including the following:

- To engage in technical maintenance, repair and management
- To meet a legal requirement to produce records and to retrieve evidence for use at arbitration
- To ensure continuity of work processes (*e.g.*, employee departs, employee gets sick, work stoppage occurs etc.)

- To improve business processes and manage productivity
- To maintain control over our business processes, including preventing misconduct and ensuring compliance with the law

The College only accesses information stored on its system for these and other legitimate purposes, but given the College System is a work system, users should have no expectation of privacy.

Use of the College System to complete tasks that are not college-related or for college-related purposes is a privilege. “Personal use” of the College System cannot interfere with the College’s need to access its system. Users should therefore understand that if they require private “personal use” of computing and communication resources they should use a personal device and not use the College System.

Enforcement and Non-Compliance

When the College suspects a violation of this policy, it may restrict a User’s access to the College System pending completion of an investigation. When the College finds a Policy violation, it may take appropriate disciplinary action up to and including discharge for employees and expulsion for students. Such actions will be taken in accordance with all policies and procedures that govern student discipline and the College’s collective agreements.

In addition to imposing discipline against an employee or student who violates this policy, the College may report suspected violations of the law to law enforcement and will cooperate with all local, national and international law enforcement agencies. The College is not responsible for steps taken by these agencies in the investigation and prosecution of public law.

The College also reserves the right to modify, disable, access or delete College user accounts in the situation where; employee departs, employee gets sick, work stoppage occurs, etc.