FLEMING

Policy Title:	**Information Technology (IT) Appropriate Use Policy (AUP)**
Policy ID:	#6-601
Manual Classification:	Section 6 – Information Technology
Approved by Board of Governors:	June 2023
Original Approval Date:	September 1999
Effective Date:	June 2023
Next Policy Review Date:	June 2026
Contacts for Policy Interpretation:	Chief Information Officer (CIO)

1.0 - Policy Overview

Computers and other information technology (IT) resources are essential tools in accomplishing the College's mission. The College’s IT Resources are valuable assets to be used and managed responsibly to ensure their security, integrity, and availability for appropriate use in legitimate academic, administrative and research activities. Members of the College Community are granted access to these resources in support of accomplishing the College’s mission.

2.0 - Purpose

This policy establishes principles and requirements for the appropriate use of IT Resources. Additionally, this policy supports effective organizational security by protecting Users and IT Resources.

This policy is governed by and serves four (4) key principles:

1. **Ethics, Values, and Fairness -** Exercise common decency, good judgment, and respect for the members and property of the College Community.

2. **Security -** Preserve the confidentiality, integrity, and availability of IT Resources and information assets; ensuring that actions taken by the members of the College Community do not negatively affect the College.

3. **Privacy –** Protect, safeguard, and maintain the confidentiality of sensitive and personal information in the possession and/or control of the College.

4. **Compliance –** Ensure the use of IT Resources adheres to all legal, regulatory, and College policy requirements.

3.0 - Definitions and Acronyms

The following definitions and/or acronyms used in this Policy and Operating Procedure are defined as follows:

AUP: Appropriate Use Policy, this document

All Users: The set of all individuals who use IT Resources

College Community: The people who study, teach, conduct research at or work at, or under, the auspices of the College including without limitation, employees or contractors; appointees (including volunteer board members); students; visitors; and any other person while they are acting on behalf of, or at the request of the College.

CIO: The Chief Information Officer of the College who is the executive responsible for the management, implementation, and usability of information and computer technologies across the College. The CIO is further responsible for all technology solutions purchased, configured, delivered, and used across the College, ensuring high availability, functionality, information security, and privacy.

FIPPA: The Freedom of Information and Protection of Privacy Act of Ontario legislates access to information held by public institutions in Ontario subject to specific requirements to safeguard the personal information of individuals.

IT: Information Technology (IT) is the use of computers and other digital devices to create, process, store, and exchange all kinds of data, information, and electronic communications.

This includes but is not limited to computing devices and associated peripherals, wired and wireless network infrastructure, cloud infrastructure and services, all types of digital hardware and software, information and data in electronic formats, facsimile machines, scanners, telephones (analog and digital), digital storage media and other multimedia devices.

IT Standards: IT Standards are specific and granular requirements that give direction to support broader-level IT policies. Refer to the College's IT Policy Framework (#6-600) for further details.

IT Resources: Any IT systems, applications, facilities, or equipment the College owns, operates, consumes, or sources from external parties for use by the College Community.

ITS: Information Technology Services is the full name of Fleming's IT Department.

Personal Computing Device: Any computer device owned by an individual, (not the College), including without limitation a laptop, smartphone, handheld device, or tablet computer.

Personal Use: Any activity that is unrelated to the College's mission or academic, administrative, and/or research objectives.

PHIPA: The Personal Health Information Protection Act of Ontario provides a set of rules for the collection, use and disclosure of personal health information by a Health Information Custodian (HIC).

Supplier: An independent business providing value to the College (also known as a vendor, contractor, partner, consultant, or third party).

User: A person that has been authorized to interact with an IT system such as an application, device, database, website, or other Form of IT Resources.

4.0 - Scope

All members of the College Community are required to act in accordance with this AUP when using any of the IT Resources, either remotely or while on campus.

This AUP must be interpreted and applied in compliance with the College's obligations under all applicable collective agreements. Nothing in this AUP or related IT policies of the College must be interpreted as limiting or amending the provisions of any applicable collective agreement. To the extent that any such policies conflict with the College's obligations under any applicable collective agreement, such collective agreement prevails provided that its provisions do not conflict with FIPPA or PHIPA.

5.0 - General Principles

- **a)** All IT Resources are made available to authorized Users to support the College's mission and are intended for academic, administrative, and research purposes. Appropriate and acceptable use is use that is consistent with an individual's role, rights, and responsibilities at the College.
- **b)** Personal Use of IT Resources is a privilege. As such it should be kept to a minimum, conducted with due care to ensure a clear separation of personal and College data, not incur any additional costs to the College and not consume a significant amount of resource capacity.
- **c)** Any activity that could impact the fair, safe, and productive use of IT Resources or negatively impact the College's operations, assets, and/or reputation is prohibited.
- **d)** Individuals are required to conduct themselves in an appropriate professional manner exercising good judgment when using any of the IT Resources.
- **e)** Users are accountable for all activities logged against their account(s), their assigned devices, and their secure electronic signature, including any misuse or illegal activity.
- **f)** Any use of IT Resources implies that the User has read and understood this AUP and agrees to abide by all terms and conditions.

5.1 – Appropriate Use

Users with access to the IT Resources must agree to and accept the following:

To comply with provincial and federal laws and regulations and abide by all College policies, operating procedures, standards, and contractual obligations when using any of the IT Resources.

To protect their College-assigned IT account(s) and related authentication mechanism(s) (such as passwords, multi-factor authentication (MFA) devices, key-based credentials, etc.) from unauthorized use.

To only use accounts, passwords, or any access credentials that have been authorized for their use within their current role at the College.

To only access and use IT Resources they are authorized to do so and only in the manner, purpose, and extent authorized. The ability to access IT Resources does not, by itself, imply authorization to do so.

Comply with the College's IT security controls, practices, and College Policy #6-604 Electronic Information Security Policy.

Comply with intellectual property rights, copyrights and College Policy #9-903 Intellectual Property.

Comply with licensing and contractual agreements related to IT Resources.

5.2 – Inappropriate Use

Inappropriate use includes and is not limited to the following list. Users are not permitted to:

a) Engage in activities that violate federal or provincial laws or regulations, or College policies. Specifically, except as permitted by this AUP, and without derogating from all other obligations of this AUP, activities that are in violation of federal or provincial laws or regulations and/or College policies include without limitation using or attempting to use IT Resources:

- **i.** to: (1) pirate software; (2) access material that is illegal, or that advocates or facilitates illegal acts; (3) access technology that is considered a controlled good under federal law on an unencrypted connection; (4) commit criminal harassment, hate crimes, or libel and defamation; (5) commit theft or fraud; or (6) violate child pornography criminal laws;
- **ii.** for transmitting, retrieving, creating, downloading, or storing any communication, file or information that is: (1) discriminatory, harassing, threatening or advocating violence; (2) promoting hatred or contempt of any group or class or persons; (3) defamatory, libellous, abusive or threatening; (4) encouraging of conduct or engaging in conduct that would constitute a criminal offence; (5) an infringement of copyright, trademark, trade secret or other intellectual property rights; (6) in furtherance of an

unauthorized access of accounts, files, programs, communications or information or (7) in violation of any license governing the use of software or third party intellectual property rights;

   iii. to: (1) engage in academic dishonesty or plagiarism; (2) engage in discrimination and harassment, including making threats, stalking, or distributing malicious material; or (3) direct others to breach any provision of this AUP; and

   iv. for transmitting, retrieving, creating, downloading, or storing any communication, file or information that is: (1) encouraging of conduct or engaging in conduct that would give rise to liability of the College; (2) misrepresenting or misleading with regards to the sender's identity; (3) in furtherance of an unauthorized access of accounts, files, programs, communications or information; or (4) a collection, use or disclosure of any personal information contrary to the College's privacy policy.

b) Share passwords or other personal authentication details with another person thereby providing unrestricted access to their personal College user account. (Students choosing to include parents/guardians in communications with the College that contains personal information about the student can do so by submitting a Student Authorization for Release of Personal Information to Third Party Form).

c) Circumvent, attempt to circumvent, or assist another in circumventing the security controls in place to protect IT Resources and College data.

d) Knowingly download or install unauthorized software onto IT Resources, which does not meet College IT security or licensing requirements or does not have a clear business or academic use.

e) Engage in activities that disrupt or interfere with other Users or IT Resources.

f) Intentionally distribute viruses or other malicious code or install software or hardware that permits unauthorized access to IT Resources.

g) Access IT Resources for which authorization may be erroneous or inadvertent.

h) Conduct unauthorized network scanning of IT Resources.

i) Conduct dissemination of unsolicited and unauthorized electronic communications, also known as email spam.

j) Physically connect a device to the Fleming hard-wired ethernet network unless expressly authorized to do so by a member of the ITS. (The use of College wireless/Wi-Fi is allowed as well as physical audio/visual (AV) connections to user-facing AV input ports, such as those provided at lecture podiums or in meeting rooms.)

k) Engage in excessive use of IT Resources, including but not limited to network, storage, and service capacity. Excessive use means use that is disproportionate to that of other Users, the intended capacity use for College purposes, is unrelated to academic or employment-related needs or negatively interferes with authorized uses. (Also see General Principle (b) regarding minimal Personal Use.)

Employees of the College are not permitted to:

- **a)** Use their home/personal email accounts to conduct College business. This is to protect home/personal resources from potential exposure to freedom of information requests.
- **b)** Use any home/personal communication resources, such as a home phone number, to communicate with students or Suppliers.
- **c)** View or distribute harassing, defamatory, discriminatory, pornographic or hateful material and messages, using IT Resources, unless such prohibition infringes upon academic freedom.

5.3 – Conflict of Interest

In general, any use of IT Resources for personal, commercial or financial gain or for political causes is considered to be a conflict of interest and in violation of this policy and the College's Conflict of Interest Policy (#3-344), unless the employee/student making such use has filed a Disclosure of Conflict of Interest to the College as outlined in the Conflict of Interest Operating Procedure (#OP 3-344) and received formal approval from the College to engage in such use.

5.4 – Copyright and Intellectual Property

The use of the IT Resources to engage in activities that violate the Copyright Act, the College's Copyright Policy (#9-904) or Intellectual Property Policy (#9-903) is strictly prohibited. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

The College recognizes that current intellectual property laws do not protect all forms of Indigenous traditional knowledge. The College commits to recognizing these differences and supporting the rightful Indigenous ownership over cultural heritage, traditional knowledge and traditional cultural expressions on its campuses. This includes the collection and storage of data as it relates to Indigenous people, community and knowledge. Refer to College Intellectual Property Policy (#9-903) for more details.

5.5 – Harassment and Discrimination

In accordance with the College's Harassment and Discrimination Prevention Policy (#3-311), any use of the IT Resources that may violate a person's right to work and study in an environment free from discrimination and harassment is strictly prohibited.

5.6 –Acquisition of IT Services and Resources

The purchase or acquisition of any IT service or resource on behalf of the College must be made under the direction and approval of the ITS. As determined and required by the ITS, privacy, security, and technical reviews will be conducted for IT goods or services, prior to procurement and/or use. Software, whether free or paid, must be approved by ITS to appropriately assess and manage any data/information risk to the College.

The only exception to the above policy statement is the purchase of low-cost (under $500 total order value) consumable hardware items.

All IT Resources acquired by the College are the property of the College and will be operated, maintained, and administered by the ITS, individuals authorized by ITS to do so, or otherwise as directed by the CIO, on behalf of the College to maximize its benefits.

5.7 – Information Management

a) All College electronic records related to College business must be in possession of the College and stored on an approved IT Resource owned and/or operated by the College.

b) All College electronic records produced by employees in the normal course of operations belong to the College. Employees of the College are responsible for maintaining accessible records and information in accordance with College policies and procedures, and relevant provincial and federal legislation.

c) Users must only share College data with others as allowed by applicable policies and procedures, and dependent on their assigned role.

d) Users must protect the confidentiality of information that belongs to the College, its students, employees, partners, and Suppliers, in accordance with the requirements of relevant provincial and federal legislation, contractual restrictions, and related College policies and procedures.

e) Users are responsible for the proper management and handling of information in accordance with related provincial and federal legislation, the College's Information Security Classification Procedure (#OP 6-604A), and the College's Access Control Procedure (#OP 6-604B) and all other College policies.

f) During the performance of an employee's duties and responsibilities, they are prohibited from storing sensitive College information and records on a Personal Computing Device unless they have been granted specific permission to do so.

5.8 – IT Security

Protection of the College's records, electronic information, and IT Resources are responsibilities shared by all members of the College Community. At all times, all Users must:

a) Abide by the College's Electronic Information Security Policy (#6-604), related operating procedures, and the College's IT Standards.

b) Contact the IT Service Desk immediately in the event of a suspected information security incident. Refer to Operating Procedure #6-604C, Information Security Incident Management for further information.

c) Never disclose any component of sensitive information unless the recipient owns or is authorized to have access to the information.

d) Keep secret authentication information such as passwords/passphrases, PIN codes, or any other authentication information secure and at no time share personal authentication information with any individual.

e) Under certain technical circumstances, members of the ITS or other Fleming System/Application Administrators may need to set a temporary user password as part of account creation, reset or recovery processes. In these scenarios, the password shall be considered temporary confidential information that requires a forced change by the user upon first login, (if this administrative feature is available), or manually changed by the user as soon as possible after receiving it.

f) Take precautions before opening any attachments or clicking on links within electronic messages.

g) Only use the College-provided secure remote access tools when performing work remotely.

h) Only use third-party cloud services or applications to conduct College business that have been approved by the ITS for specific uses and have been subject to the ITS third-party vendor risk assessment.

i) Ensure that Personal Computing Devices that may come in contact with IT Resources or College information are password protected, protected with antivirus software and a device-level firewall, and have consistently applied software updates and patches to operating systems, applications, and web browsers.

5.9 – Privacy

The College respects the privacy of its students, employees, Suppliers, and guests and will not access, use, or disclose personal user data or information without cause. Refer to College Policy #1-111 Access to Information and Protection of Privacy for more details.

5.10 - IT Resources Health and Usage Monitoring

Notwithstanding the terms of Section 5.9, the College has the duty to conduct IT Resources health and usage monitoring, as deemed necessary at its sole discretion, to protect the security, confidentiality, integrity, and availability of the College’s IT Resources. All IT Resources are actively monitored and logged for security, diagnostic, and audit purposes, including User actions. By using IT Resources, the User grants the College permission to collect, use, access, and disclose their personal user data for purposes permitted under this AUP. Users who engage in Personal Use of IT Resources are deemed to accept that the College has a right of access and may raise no expectations of privacy that prevents the College from accessing and using information and data for purposes permitted under this AUP.

Exceptions to user privacy and subsequent data access may occur for the following reasons:

a) To engage in technical maintenance and repair;

b) To protect and maintain IT Resources or other assets and interests, from an immediate or imminent threat;

c) In support of the College’s efforts to comply with legal requirements, or defend itself in proceedings, to meet a legal requirement to produce information, including by e-discovery;

d) To prevent misconduct and ensure compliance with the law; and

e) To fulfill other legitimate business, corporate, or human resources purposes, including because of the absence of an employee to ensure continuity of work.

As part of IT Resources health and usage monitoring, the College may:

- **a)** recover deleted files and data stored or accessed using IT Resources;
- **b)** filter and quarantine both inbound and outbound content and network traffic; and
- **c)** log system activities and user actions for the purposes of technical diagnostic, security, and information integrity.

5.11 - User Monitoring

Notwithstanding the terms of Section 5.9, the College reserves the right to conduct User activity monitoring of IT Resources. The College may exercise this right if, in the opinion of the CIO (or designate), there are reasonable grounds and/or a reasonable belief based on credible information received to support User monitoring, including information or belief that:

- **a)** The results from general IT Resources health and usage monitoring provide reasonable grounds to focus on and review a specific User's activity. (e.g., security monitors flag that a User's account is suspected of being compromised based on the User's login history, location(s), or other correlated activities.)
- **b)** A User is violating this AUP or any other College policies, or any relevant federal and provincial legislation in their use of IT Resources.
- **c)** A User is using IT Resources in a fashion incompatible with their employment with the College.

5.12 – Compliance and Enforcement

- **a)** Pending an investigation, the College reserves the right to immediately suspend a User's access to any and all IT Resources.
- **b)** Subject to the collective agreements of the College, if applicable, employees and students at the College who violate this AUP may be subject to disciplinary action up to and including termination of employment or expulsion.
- **c)** Suppliers and guests who violate this AUP may have their College contracts terminated and/or be refused all future entry to College campuses.
- **d)** The College reserves the right, at its discretion, to permanently revoke student, employee, Supplier, or guest access to all IT Resources at any time.
- **e)** Users who violate municipal, provincial, federal, or international law may be subject to criminal prosecution and/or civil litigation by the appropriate authorities.

6.0– Responsibilities

6.1 – User

- **a)** Review, understand and comply with policies, laws and contractual obligations related to access, appropriate use, and the security of IT Resources.
- **b)** Consult with the ITS on appropriate use issues not specifically addressed in this AUP.
- **c)** Protect personal information and personal assets used to access personal information or College data.
- **d)** Report any suspected violations of the AUP to the ITS Service Desk or CIO (or

designate), depending on the level of confidentiality and severity of the suspected incident. For more information see the College's Information Security Incident Management Operating Procedure #6-604C.

6.2 – Chief Information Officer

a) Designate individuals who have the responsibility and authority for IT Resources.
b) Designate individuals who have the responsibility and authority for monitoring and managing IT Resources.
c) Designate individuals who have the responsibility and authority for investigating alleged violations of this AUP.

7.0 – Related Documents

- *Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F. 31*
- *Copyright Act (Canada) R.S. 1985*
- College Policy #1-111, Access to Information and Protection of Privacy
- College Policy #2-201A, Academic Integrity
- College Policy #3-311, Harassment and Discrimination Prevention Policy
- College Policy #3-344, Conflict of Interest Policy
- College Policy #4-403, Computer Software, Copyright
- College Policy #5-506, Student Rights & Responsibilities
- College Policy #6-600, IT Policy Framework
- College Policy #6-604, Electronic Information Security Policy
- College Policy #9-903, Intellectual Property
- College Policy #9-904, Copyright
- Operating Procedure, #OP 3-344, Conflict of Interest
- Operating Procedure #6-601, AUP and accessing another user's data
- Operating Procedure, #6-601A, Remote Access
- Operating Procedure, #6-604A, Information Security Classification Procedure
- Operating Procedure, #6-604B, Access Control Procedure
- Operating Procedure, #6-604C, Information Security Incident Management

8.0 - History of Amendments/Reviews

Date	Actions
September 1999	Originally approved
November 2008	Reviewed and updated
May 2013	Reviewed and updated
June 2023	Reviewed and updated