SIR SANDFORD FLEMING COLLEGE POLICY MANUAL

Policy # 6-601 Information and Communications Technology (ICT) Appropriate Use Policy	
Classification: *Section 6 – Information Technology Services*	
Approved by: Board of Governors	Date: May 1, 2013 (BoG May 1, 2013 #2)
Replaces: # 6-601 (BoG Nov 26, 2008 #8; BoG Sept 1, 1999 #9)	
Next Policy Review: 2018	Responsibility*:* Executive Leaders Team

Policy Statement

This policy provides a framework for the appropriate use of Information and Communications Technology (ICT) services/resources/equipment and facilities at Fleming College. Individuals using ICT services/resources/equipment and facilities at Fleming College are responsible for reading, understanding, and observing this policy.

Purpose

This policy balances the need for a high level of access, flexibility and protection of privacy for users, with the need for a framework that provides Information Technology staff and the College with the ability to respond to alleged policy violations as they arise and to protect institutional interests.

Scope

This policy applies to everyone with a Fleming College IT Network user account.

The primary office of responsibility for this policy is the Chief Information Officer.

Definitions

AUP: Appropriate Use Policy

CIO: Chief Information Officer

ICT: Information and Communications Technology; it includes software and systems used for academic delivery and administrative purposes either hosted at college facilities or in third party premises**,** all of the information stored in systems, computing devices and associated peripherals, VoIP communications network and wireless infrastructure and related equipment, facsimile machines, scanners, telephones, wireless devices, digital storage media, video and other multimedia devices.

General Principles

Fleming College is committed to ensuring a working and learning environment in which all ICT users have the responsibility to respect the physical and emotional well-being, and the sense of personal worth and dignity of others in the college community, as well as promoting the responsible and ethical use of college resources.

ICT services and resources provided at Fleming College are intended for teaching, research, and administrative purposes.

Use of ICT is governed by all applicable College policies, including Harassment and Discrimination Prevention, Freedom of Information and Protection of Privacy (Bill 34), Software Copyright, Student Rights and Responsibilities, Residence-Reznet guidelines, as well as by all applicable Canadian federal, provincial and local laws and statutes, including the Criminal Code of Canada and the Ontario Human Rights Code. These are supplemented by various rules and guidelines adopted in specific academic and administrative units.

Operating Procedure

1.0 ICT AND COMMUNICATION

1.1 Confidentiality

The College believes that each individual has a right to privacy. No person, regardless of status may view or change or remove another user's electronic files or data without the user's permission, whether the material exists on a shared computer, network media or on a user's personal media.

The College ICT Network is provided for the use of authorized persons, but remains the property, and within the control of Fleming College. The use of this business and educational system for personal reasons is a privilege. The College believes that each individual has a right to privacy. No person, regardless of status may view or change or remove another user's electronic files or data without the user's permission, whether the material exists on a shared computer, network media or on a user's personal media. By using a password protected account, users are not anonymous and deleted user data may be retrieved and/or restored from system backups. Exceptions to user privacy and subsequent access to user data exists as follows:

- To engage in technical maintenance repair and management
- To meet a legal requirement to produce information, including by e-discovery
- To ensure continuity of work (e.g. employee is sick or injured and work needs to be retrieved)
- To prevent misconduct and ensure compliance with the law

In such cases access to personal data shall only be given with due diligence of requesting such access via the CIO or in their absence a delegated authority.

Note: non-personal information such as IP address may be used to investigate and understand the system usage patterns, and/or functionality.

1.2 Pornography, Hate Literature, and Cyber-bullying

ICT resources are not to be used to create, transmit, store or copy information that is threatening, harassing, illegal or incites hate.

1.3 E Mail Communications

The College Harassment and Discrimination Prevention and Student Rights and Responsibilities policies pertain to these communication media.

1.4 Web/Internet Communications

Complaints about threatening, harassing, or illegal content or content that incites hate, that is created, transmitted, stored or copied using Fleming ICT resources and distributed on the Internet or any other external system, will be investigated as possible violations of the Appropriate Use Policy. This includes content that could be considered defamatory or damaging to the institution's public image.

1.5 Network Printing, Scanning, Fax and VoIP Voice Communications

These devices are considered communication media, and as such, all relevant policies and procedures will apply to them. Communication using the VoIP phone system is part of the ICT Network and thus the Appropriate Use Policy applies.

2.0 SECURITY

2.1 User Account Security

Every user of the Fleming ICT network and facilities has a responsibility to ensure the security of the network, information, data and resources. It is the responsibility of the individual user to maintain the security of her/his account by choosing a secure password, not disclosing/sharing passwords and to take reasonable steps to prevent unauthorized access. Users are expected to change their initial default password to a confidential, secure password. Employees are required to report instances where they become aware of any unauthorized use of ICT.

Information Technology staff will disable an account if there is some indication that the security of the account or network has been breached.

2.2 Network Security

Information Technology Services staff are the only staff authorized to plug devices into the Fleming ICT network. Special requests for one-time unique connections that require unique or special configuration must be approved by Information Technology Services. Information Technology Services staff will only interconnect physical network drops which have been provisioned through the formal process of adding/ moving infrastructure to the Fleming ICT Network. Wireless access to the Network will be provisioned through formal processes developed and maintained by the Information Technology Services Department that meet the needs of the user and maintain network security. The Information Technology Services Department also has the right to terminate any process when deemed necessary, in order to maintain network system integrity.

2.3 Information and Data Security on Portable ICT Devices

Fleming employees should avoid copying and transporting college data on portable storage devices, in particular data which contains personal information. If a user has to copy and transport college data, the individual employee has a responsibility to ensure that any college information and data stored on portable devices including, but not limited to laptops, notebooks, PDAs, USB keys, and external digital storage devices de-identifies personal information, is encrypted and secure at all times.

Upon disposal of the portable device the user is to ensure that any copied data on the device must be deleted or erased as soon as it is no longer needed, using appropriate measures to prevent unauthorized access to college information.

2.4 Viruses

Individuals are responsible for any damage to their work, data and files due to viruses they have introduced, either intentionally or unintentionally. The College is not responsible for any work, files or data which are lost, damaged and/or destroyed due to viruses introduced onto the network.

2.5 Spam

Production or facilitation of Spam is a violation of this Appropriate Use Policy.

2.6 Firewall

Network Firewalls are provisioned for the protection of all users and deliberate attempts by any user to bypass the normal operation of the firewall or Intrusion Detection and Prevention Systems by either technical or physical means is a violation of the Appropriate Use Policy.

Users should be aware that during the regular course of carrying out their duties, Information Technology staff may from time to time inadvertently view the content of data packets leaving or entering the college network via the firewall.

2.7 Remote Access to Fleming College Network

Once a user accesses the Fleming ICT network remotely, this Appropriate Use Policy applies to their usage.

3.0 PHYSICAL FACILITIES SECURITY

ICT equipment is the property of the College. No person or persons will, by any willful or deliberate act, jeopardize the integrity of ICT equipment, systems software programs or other stored information and data. Any action or attempt by a user to subvert or disrupt the functioning of any ICT equipment is prohibited.

4.0 SOFTWARE SECURITY

Software and personal files are intellectual property and thus are subject to copyright law. Installation and/or extraction of software on the Fleming ICT Network are subject to the applicable software license. The College will assist any software supplier with just cause, to prosecute any individual violating software copyright laws. It is the responsibility of users to familiarize themselves with their responsibilities and limitations under each End User License Agreement (EULA).

Users must not attempt to:

i) Access and use software belonging to or licensed to other users or to Fleming College without proper authorization to do so.

ii) Move or copy programs, subroutines and any other forms of software from one computing system to another without proper authorization.

iii) Install or use software on the Fleming ICT Network for which the user does not have authorization under the EULA.

iv) Distribute, sell or otherwise make available software when such activity is prohibited by the license agreement for that software.

v) Access data or information stored on College-owned computers without the permission of the owner or custodian of that information.

5.0 FLEMING COLLEGE ICT INFRASTRUCTURE SUPPORTED WEBSITES

Employee and student information is protected under the Freedom of Information and Protection of Privacy Act. When posting materials that could be accessed via the Portal or external website, authors will comply with FOI and copyright requirements along with college approved design standards.

6.0 ICT SOFTWARE/HARDWARE ACQUISITION

All ICT purchases for the College must be coordinated with the Information Technology Department. All ICT resources acquired by the College are the property of the College and will be operated, maintained and administered by the College to maximize its benefits.

7.0 ACTIONS TO BE TAKEN ONCE A POTENTIAL AUP VIOLATION HAS BEEN REPORTED

1) The CIO or designate confirms that there is a real or potential violation of the AUP.

2) Through phone or email a request is made to the appropriate IT staff to immediately disable access to the user's account. If the request is made via the phone it must be followed up by a documented request by email within 12 hours. The user account will be flagged and an AUP violation number is created. The AUP violation log is updated to include:
   - AUP violation number
   - Date and time of reported violation
   - Person reporting the violation
   - A brief description of the user behaviour or reason that lead to the suspicion or allegation of violation.

- Any other information relevant to the specific incident.

3) A copy of all activity (fata, files, browser history, login history, desktop activity) associated with the account is produced and stored in an alternate, secure location.

4) In the case of an alleged employee AUP violation the supervisor will be contacted.

5) In the case of an alleged student AUP violation the procedures through the Student Rights and Responsibilities Policy will be invoked.

8.0 RESPONSIBILITIES

8.1 Individual Users

Responsible use of ICT services and facilities require that users:

i) Respect the legal protection provided by copyright and license to programs and data.
ii) Respect the rights of others by complying with copyright laws regarding intellectual property.
iii) Respect the rights of others by complying with the College's Harassment & Discrimination Prevention Policy.
iv) Respect the rights of others by preserving the privacy of personal data to which they have access.
v) Respect the integrity of ICT systems and data; for example, by not intentionally developing programs or making use of already existing programs that harass other users, or infiltrate a computer or computing system, and/or damage or alter the software components of a computer or computing system, or gain unauthorized access to other facilities accessible via the network or web.
vi) Use ICT facilities in a manner which is consistent with the ethical principles set forth by the College.
vii) Respect and adhere to any local, provincial or federal law which may govern use of these information and communication technology facilities in Canada. These include, but are not limited to, the Criminal Code of Canada, the Ontario Human Rights Code, the Ontario Freedom of Information and Protection of Privacy Act.
viii) Must not attempt unauthorized access to ICT installations outside of Fleming College using Fleming's ICT facilities.
ix) Use ICT resources at all times in a manner that is consistent with the College's best interests, this Policy and all applicable laws.

8.2 Chief Information Officer or Designate

Serves as the College ICT Complaints and Hearing Officer and ensures that any inappropriate use of the Fleming ICT is dealt within a timely and efficient manner.

8.3 Director, Information Technology or Designate

Responsible for reviewing all ICT based technology plans and proposals to ensure that they are compliant with international standards and ICT principles established at Fleming College, and that they can subsequently be implemented.

Related Documents

- *Harassment and Discrimination Prevention,* Policy #3-311
- *Student Rights and Responsibilities,* Policy #5-506
- Freedom of Information and Protection of Privacy legislation
- Software Copyright
- Residence Reznet Guidelines

Appendices

N/A

Monitoring of Operating Procedure

Next Review: *2016*
Responsibility of: *Chief Information Officer*

Procedure Review Summary:

Section and Month date, year	Person/Department/Committee
Section and Month date, year	Person/Department/Committee