IT Policy of the college

1. Introduction

College promotes the use of information technology to enhance its teaching, learning and working environments. Ensuring the responsible, efficient and ethical use of information technology is a community endeavor shared between staff, students and faculty.

2. Purpose

This policy provides a framework to guide users in decision-making about the usage of information technologies provided by and/or operated at College.

3. Definitions

3.1. Information Technology (IT)

Information Technology (IT) includes, but is not limited to: computer systems; networks; data storage media; software applications; hardware; or any other electronic or telecommunications media used for the digital transmission of information, on campus or remotely, through which College provides access or is connected.

3.2. User

User refers to any person who accesses the college's information technology such as students, faculty, staff, volunteers and guests.

3.3. User account

User Account refers to the privilege and/or permission granted to a specific user to access a particular portion of the college's information technology.

4. Policy statements

4.1. The primary purpose of information technology is for college-related activities including, but not limited to teaching, learning, research and administration.

4.2. The use of information technology resources is a privilege and not a right.

4.3. Information Technology users shall be aware of, and adhere to, the requirements of all federal and provincial legislation and regulations, as well as the college's policies and procedures.

4.4. Employees are expected to store their college e-mail only on college-assigned devices and/or computers.

4.5. A user account may only be accessed by the user to whom the account was assigned and only to fulfill their role unless otherwise stated in this policy.

4.6. Users need to safeguard their user passwords and not disclose their passwords to others.

4.7. As a condition of access to information technology, users are individually accountable for any authorized or unauthorized use, misuse or illegal use.

4.8.   Users need to take reasonable precautions to protect and secure college-owned and/or their own IT devices such as desktop computers, laptops and tablets.

4.9.   Users must not attempt to circumvent any security or control measures implemented on college systems.

4.10.   College shall treat all electronic communication as private and secure but this cannot be guaranteed.

4.12.   Occasional personal use of information technology is permitted provided such use does not hinder the work or resources of the user or others.

4.13.   Examples of unacceptable use
• For illegal purposes;
• To interfere with or disrupt network users, services, equipment, either within or outside the college;
• To gain unauthorized access to hardware or software resources, either within or outside the college;
• Storing college business e-mail(s) on personal computers, phones or Personal Digital Assistants (PDAs) that are not college assets;
• For business or political reasons, which are not directly in support of learning or the administration of the college;

• To post or transmit messages considered as 'spam', which includes but is not limited to bulk unsolicited messages or inappropriate postings to newsgroups or social media;
• To distribute unsolicited advertising unless prior approval is received from the college;
• Unauthorized copying, removing or distributing proprietary software and data;
• Decompiling, disassembling, modifying, translating or otherwise reverse engineering software to discover any source code or underlying algorithms of the software;
• To intentionally transmit, receive or display threatening, obscene, hate, and anonymous or harassing materials (cyber-bullying); and
• To knowingly propagate computer worms or viruses or other disruptive or destructive constructs.

5. Roles and responsibilities

5.1 Coordinator is responsible for ensuring that this policy is fully implemented.

5.2 A detailed description of roles and responsibilities relating to this policy is provided in the Acceptable Use of Information Technology Procedure.

6. Coordinator is responsible for enforcing the policy. Non-compliance implications Failure to comply with this policy could result in loss of access to College information technology services and equipment, suspension or termination of an employee or academic studies.

7. Related policies, procedures and directives

• All the policies related to the college.