Durham College Policy and Procedure

TYPE:	Administrative
TITLE:	Acceptable Use of Information Technology
NO.:	ADMIN-206
RESPONSIBILITY:	Chief Information Officer and Associate Vice-President, Information Technology
APPROVED BY:	Durham College Leadership Team
EFFECTIVE DATE:	December 2016
REVISED DATE(S):	
REVIEW DATE:	December 2019

1. Introduction

Durham College promotes the use of information technology (IT) to enhance its teaching, learning and working environments. Ensuring the responsible, efficient and ethical use of IT is a community endeavour shared between employees and students.

2. Purpose

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

3. Definitions

Refer to Durham College's Standard Definitions.

4. Policy statements

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

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

4.3. IT 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 email 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.

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

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

4.9. 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.

4.10. Users must not attempt to circumvent any security or control measures implemented on College systems.

4.11. Durham College considers any violation of this policy to be an offence and reserves the right to copy and examine any files or information resident on College systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten to degrade operations. Where relevant, a user's privileges may be suspended during the investigation of an unacceptable use incident.

4.12. Users found to have breached this policy and procedure may be subject to College and/or legal actions. Penalties may include, but are not limited to warning (no record); warning (written record); conduct contract; immediate, temporary and/or permanent loss of information technology privileges; restitution; probation; restriction of access to College facilities; temporary dismissal from the College; and permanent dismissal from the College. Offenders may also be prosecuted under federal, provincial and municipal laws, regulations and by-laws.

4.13. Durham College shall treat all electronic communication as private and secure but this cannot be guaranteed. Users should not have an expectation of complete privacy when using IT.

4.14. Occasional personal use of IT is permitted provided such use does not hinder the work or resources of the user or others.

4.15. Users observing any breaches of this policy shall make a report to the IT Security Officer.

4.16. Breaches of the this policy include, but are not limited to: the circumvention or compromise of security systems; excessive use that interferes with the resources of others; destruction or disruption of data, networks or equipment; copyright infringement; patent infringement; intellectual property rights infringement; unauthorized deletion, modification, use or monitoring of information; violations of privacy; or the operation of a personal for-profit enterprise.

4.18. 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.
- The foregoing list is illustrative and should not be construed as exhaustive. Please ask the IT Security Officer for clarification if unsure about whether a planned use is acceptable.

5. Procedure

5.1. User IT Security Responsibilities

5.1.1. Users need to take reasonable precautions using available means to protect and secure their IT devices especially those containing confidential data.

a) Where technically feasible, all devices including computers will be password protected. Please reference the password standards in the following section.

b) Users will ensure that this password protection remains in place at all times.

c) Users need to use malware and virus protection, provided by the College on College owned IT equipment.

d) Non-College owned equipment accessing College IT should use security safeguards such as malware and virus protection.

e) Users should keep their IT devices in secure places to prevent theft.

5.1.2. If a user suspects that their College owned IT device has been compromised, and is infected, s/he needs to report it to the IT Service Desk and request support from the IT Service Desk.

5.2. Password Standards

5.2.1. Secure Passwords

Passwords need to be secure, changed regularly at least every 120 days, and not shared with others. Secure passwords should be of sufficient complexity that these cannot be easily guessed. To ensure a password is secure it needs to be 8 characters or longer and comprised of a combination of mixed case letters, numbers and symbols. An example could be a name or phrase, modified slightly, like "b0b$mith" or "M@ryL0ng".

5.2.2. Forgotten Passwords

Users need to go to the Service Desk Counter located throughout the various campuses for assistance. Campus or Government-issued photo ID will be required. If they are not able to visit the IT Service desk, they need to call 905.721.3333 for support. For security reasons, ITS cannot give out usernames and passwords by email.

5.3. Privacy Guidelines

5.3.1. All reasonable attempts have been made to ensure the privacy of user accounts and user electronic mail. This is not a guarantee that user accounts or user electronic/voicemail are private. Program and files (including e-mail/voicemail files) are confidential unless they have been made available, with the owner’s written permission, to other authorized individuals. Durham College reserves the right to access all information stored on its network and systems. Files may be released at the request of legal authorities.

5.3.2. File owners will be notified of file access and/or maintenance, in advance, if such notice is practical. However, at the discretion of the College's Chief Privacy Officer (Chief Administrative Officer) notification may be withheld if it would comprise an investigation by the College or other legal authorities. When performing maintenance every effort is made to respect the privacy of a user's files. However, if policy violations are discovered, they will be reported immediately to the appropriate College authorities and privilege will be immediately revoked until adjudication.

5.3.3. For additional information related to privacy and keeping information protected, please reference records management tip sheets on ICE.

5.4. IT Security Incident

5.4.1. All employees, students and clients are responsible for reporting all perceived infractions or potential breaches of this policy to the IT Security Officer.

5.4.2. Upon receipt of a report, the IT Security Officer will form a multidiscipline case management team to conduct a full investigation to collect information about the reported incident and determine if it could possibly be a breach of any applicable College policy, or provincial or federal laws.

5.4.3. The Office of Campus Safety will be briefed and notified of all preliminary reviews and/or any potential infractions and will determine the course of action required. When necessary, the Office of Campus Safety will conduct a full investigation.

5.4.4. Where the case management team has sufficient information that the incident could be a breach, the team will communicate in writing the specifics of the case and actions taken to the individual being investigated, including, if warranted a decision to have ITS temporarily suspend access to all IT privileges until such time as the investigation is completed. The team will also communicate to the appropriate vice-president.

5.4.5. The Chief Information Officer is responsible for the decision to temporarily disable and then restore IT privileges. All decisions to disable or restore IT privileges must be made in writing to the individual being investigated.

5.4.6. Suspension of access to all IT privileges will remain in effect until such time as the investigation is completed, penalties are lifted or an appeal has been made and adjudicated.

5.5. Disciplinary action

Following the completion of the investigation, where incidents are found to be in violation of College policy, provincial or federal law, the College will exercise its rights to take appropriate action, including, but not limited to:

- A verbal and written warning;
- Restrictions, temporary or permanent removal of access to any or all institution computing facilities and/or services;
- Legal action that could result in criminal or civil proceedings;
- Disciplinary directives, behavioral contracts, suspension and/or expulsion/dismissal from the College; and/or
- The incident, decision and any disciplinary action will be filed in the student or employee's file.

6. Roles and responsibilities

6.1. Students and employees are responsible for safeguarding and controlling the use of assigned IT access privileges and IT devices, and adhering to the procedure and reporting perceived breaches of this policy.

6.2. The IT Security Officer is the first point of contact for reported security breaches, and leader of the investigation procedure. The Manager, IT Service Management and Governance fills this role.

6.3. The Chief Information Officer is responsible for disabling or restoring all access to College IT resources, and monitoring this policy and procedure according to an established schedule, or more frequently in response to feedback from the College.

6.4. The Vice-President, Academic participates in the decision to disable a student's or faculty member's access and all communications, and is responsible for monitoring this policy and procedure according to an established schedule or more frequently in response to feedback from the College.

6.5. The Chief Administrative Officer and the Vice-President, Student Affairs participate in the decision to disable access and all communications to their respective employees, and they are responsible for monitoring this policy and procedure according to an established schedule more frequently in response to feedback from the College.

6.6. The Office of Campus Safety will determine course of action and complete an investigation if needed.

7. Accessibility for Ontarians with Disabilities Act considerations

Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this policy and procedure and it adheres to the principles outlined in the College's commitment to accessibility as demonstrated by the Accessibility Plan (ADMIN-203).

8. Non-compliance implications

Failure to comply with this policy and procedure could result in loss of access to Durham College information technology services and equipment, suspension or termination of an employee or academic studies.

9. Communications plan

- A message will be posted on ICE alerting employees when new or revised policies and procedures are added to ICE.
- A message will be posted on MyCampus alerting students when new or revised policies and procedures are added.

10. Related forms, legislation or external resources

None.