College Procedure

PROCEDURE TYPE:	Administrative
PROCEDURE TITLE:	Acceptable Use of Information Technology
PROCEDURE NO.:	ADMIN-206.1
RESPONSIBILITY:	Chief Information Officer & 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 to enhance its teaching, learning and working environments. Ensuring the responsible, efficient and ethical use of information technology is a community endeavour shared between staff, students and faculty.

2. Definitions

2.1. 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 Durham College provides access or is connected.

3. Procedure

3.1. User IT Security Responsibilities

3.1.1. 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 thereof.

3.1.2. 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.

3.2. Password Standards

3.2.1. 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". Examples can be found at http://servicedesk.durhamcollege.ca

3.2.2. 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.

3.3. Privacy Guidelines

3.3.1. 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.

3.3.2. 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.

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

3.4. IT Security Incident

3.4.1. All employees, students and clients are responsible for reporting all perceived infractions or potential breaches of the Acceptable Use of Information Technology Policy to the IT Security Officer.

3.4.2. 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.

3.4.3. 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.

3.4.4. 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.

3.4.5. 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.

3.4.6. 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.

3.5. 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, behavioural 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.

4. Roles and responsibilities

4.1. 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.

4.2. 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.

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

4.4. 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 procedure according to an established schedule or more frequently in response to feedback from the college.

4.5. 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 procedure according to an established schedule more frequently in response to feedback from the college.

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

5. Related policies, procedures and directives

- Durham College Student Rights and Responsibilities Policy ACAD-115 and Procedure
- ACAD-115.1
- Durham College Employee Code of Conduct Policy EMPL-317
- Durham College Acceptable Use of Information Technology Policy ADMIN-206

- Durham College Wireless and Cellular Technology Policy ADMIN 221 and Procedure ADMIN 221.1
- Durham College Moveable Information Technology Asset Policy ADMIN 216