DOUGLASCOLLEGE

ACCEPTABLE USE OF COMPUTER AND INFORMATION TECHNOLOGY POLICY

Policy Name:	Responsible Owner:	Created:
Acceptable Use of Computer and Information Technology	Associate Vice President, Technology and CIO	2017 Mar
Policy Number:	**Approval Body:**	**Last Reviewed/Revised:**
A56	SMT	2020 Mar
Category:	**Replaces:**	**Next Review:**
Administration	N/A	2025 Feb

TABLE OF CONTENTS

A. PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment and information technologies at Douglas College. These rules are in place to protect students, employees and Douglas College by eliminating or mitigating risks including virus attacks, compromise of network systems and services, and legal issues.

B. SCOPE

This policy applies to the use by any member of the College Community of information, electronic and computing devices, telephones, printing, and network resources to conduct Douglas College business or interact with its networks and business systems, whether owned or leased by Douglas College, a student, an employee or a third party.

C. DEFINITIONS

College Community: Includes all employees, students, users, contractors, suppliers, guests and any other person participating in any College-related activity or attending an event on College premises.

Confidential Information: Data classified as Level 3 (Highly Sensitive) or Level 4 (Personal and Regulated) (as per Douglas College Administration policy *A42 Information Security Policy*).

Highly Sensitive Data (classification Level 3): Data that if compromised can cause considerable harm or embarrassment to the College (as per Douglas College Administration policy *A42 Information Security Policy*).

Information Security: The state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this.

Malware: A malicious code that may exist as a file, may be embedded within legitimate computer files or websites, or may exist only in computer memory for the purpose of causing harm to a computer, data or persons. Malware may come in a form of computer viruses, worms, trojans, ransomware or file-less malware.

Personal and Regulated Data (classification Level 4): Data that if compromised could result in long-term harm or reputational risk to the College and/or to individuals, such as breach reporting, negative press, lawsuits against the College, considerable loss of revenue (as per Douglas College Administration policy *A42 Information Security Policy*).

Personal Use: Use of Douglas College technology and/or resources for purposes of a personal nature, and not required for College-related activity.

Significant Cost: An amount incurred above or outside the normal cost to the College of doing business, such as for personal use of a College cell phone that incurs charges beyond the rate for the standard plan (e.g., exceeding maximum minutes or data allowed). Discussion with a direct supervisor may be required to determine if reimbursement to the College is required.

D. POLICY STATEMENTS

1. Technology at Douglas College is provided to fulfill job functions and/or the requirements of academic study and to support a superior learning environment. When provided to members of the College Community by the College, said technology is intended for use for College-related activity.

2. The College has the following expectations of all members of the College Community with respect to their use of College technology:
    a. That they will be responsible for exercising good judgment regarding appropriate use and safekeeping of information, electronic devices, and network resources in accordance with Douglas College policies and standards, and with local laws and regulations.
    b. That they will not share their College login credentials (login name and password) with anyone.
    c. That they will ensure that all their devices connecting to the College network and/or systems are equipped with current and adequate anti-malware capabilities.

3. The College has the following expectations of all employees, including contractors, consultants, temporary and other workers, with respect to their use of and access to information and information technology at Douglas College:

a. That they will copy confidential information to portable devices and portable media only if those devices and media use encryption.
b. That they will not copy confidential information to personal email, any personal computer drive or other non-Douglas computer drive, unless appropriate approval is granted by a direct supervisor and by the CEIT Information Security team.
c. That they will not use personal email to conduct business on behalf of Douglas College.
d. That they will not auto-forward Douglas College emails to a non-Douglas email address.
e. That they will take necessary steps to stay informed on how to be cyber aware and cyber safe, including by participating in relevant training.
f. That they will not store any of their College login credentials in any system (e.g., email, spreadsheet) with exception of those approved by CEIT Information Security.
g. That they will not request and CEIT will not create generic accounts, generic mailboxes, or system accounts without appropriate approvals and without a strong business case. Generic accounts must have an accountable account owner assigned.

4. Systems access is to be granted only to authorized users on an as-needed basis and removed in a timely manner.

5. Personal use of College information technology is allowed, providing that it does not incur a significant cost and/or risk to the College, and does not interfere with or take time away from work and/or academic programming time. Use of College resources for any non-College business purpose is strictly forbidden.

6. In the event that an employee's personal use of College resources results in a significant cost to the College, the employee shall fully reimburse the College for said costs.

7. Under no circumstances is a student or an employee of Douglas College authorized to use Douglas College-owned resources to engage in any activity that is illegal under local, provincial, federal or international law.

8. Employees found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9. Students in violation of this policy may be subject to disciplinary action under the College's *Standards of Student Conduct Policy*.

10. College Administrators are responsible for ensuring that employees and others under their supervision are aware of and uphold their Information Security responsibilities.

E. PROCEDURES

Violations of this policy may constitute a Reportable Activity as defined in the College's *Protected Disclosure* (*Whistleblower) Policy* and should be reported in accordance with the procedures found in that policy.

The following internal operating procedures are set out in the identified Standard Operating Procedure (SOP):

- Generic Account, Generic Mailbox, or System Account Request

F. SUPPORTING FORMS, DOCUMENTS, WEBSITES, RELATED POLICIES

Administrative Policies

- *College Communications Policy*
- *Conflict of Interest Policy*
- *Information Security Policy*
- *Protected Disclosure (Whistleblower) Policy*
- *Standards of Student Conduct Policy*
- *Use of College Facilities Policy*

Related Standards (available on DC Connect)

- Acceptable Use of Computer and Information Technology Standard
- Authentication Standard
- Data Classification Standard
- Mobile Device Security Standard

G. RELATED ACTS AND REGULATIONS

- Canada's Anti-Spam Legislation
- *Copyright Act (R.S.C., 1985, c. C-42)*

H. RELATED COLLECTIVE AGREEMENTS

- N/A