ACCEPTABLE USE OF COMPUTER AND INFORMATION TECHNOLOGY POLICY

Policy Name: Acceptable Use of Computer and Information Technology	**Responsible Owner:** Associate Vice President, Technology and CIO	**Created:** 2017 Mar
Policy Number: A56	**Approval Body:** SMT	**Last Reviewed/Revised:** 2022 Mar
Category: Administration	**Replaces:** N/A	**Next Review:** 2027 Oct

TABLE OF CONTENTS

A. PURPOSE

The purpose of this policy is to outline the acceptable use of all computer and information technologies at Douglas College (the College). This policy confirms expectations for the use of these College Resources, including rules designed to protect Students, Employees and the 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 of College Resources by any member of the College Community.

Application of Other College Policies

Conduct that violates this policy may also violate other College policies, such as but not limited to the following:

- For the use of College computer and/or information technology for the purpose of bullying or harassment of Employees, see also Administration policies A19 *Bullying and Harassment Prevention and Response* and A59 *Human Rights*;
- For the use by a Student of College computer and/or information technology for the purpose of bullying or harassing another Student, see also Administration policy A20 *Student Non-academic Misconduct*;
- For the use of College computer and/or information technology for the purpose of issuing communications of a threatening or violent nature, see also Administration policy A16 *Violence Prevention and Response*;

- For the use of College computer and/or information technology for the purpose of issuing communications of a sexually threatening nature, see also Administration policies A53 *Sexual Violence and Misconduct Prevention and Response* and A59 *Human Rights*; and
- For the use of College computer and/or information technology in the commission of legal wrongdoing, including fraud or financial irregularity, see also Administration policy A43 *Protected Disclosure* (*Whistleblower)*.

C. DEFINITIONS

College Community: All College Employees, Students and Board members, and any other person who is contractually obligated to comply with College policy.

College Resources: Any facilities, equipment or financial aid provided or administered by the College, including without limitation any facilities, physical structures, classrooms, research laboratories, equipment, technical facilities, personnel and services of the College, including the administration of funds received by the College in the form of grants, contracts or any other support provided by the College, affiliated agencies, partners or external sponsors; for the purposes of this policy, includes all hardware (e.g., electronic and computing devices, telephones, printing and network resources) and software made available by the College for the conducting of College business, whether that hardware or software is owned or leased by the College, and proprietary information of value to the College.

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

Contractor: A person or company that undertakes a contract to provide materials or labour to perform a service or do a job.

Employee: A person who is employed by the College, including administrators, faculty members, staff and Contractors, and Students when employed by the College (e.g., as Student Assistants or Peer Tutors).

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*).

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

Least Privilege Principle: The principle that individuals (and systems) are granted only those privileges that they need to perform their work tasks and job functions, including the ability to perform an action, such as accessing information directly within a system.

Malware: A malicious code that may exist as a file, may be embedded within legitimate computer files or websites, may exist only in computer memory for the purpose of causing harm to a computer, data or person, and/or may come in the form of a computer virus, worm, trojan or ransomware, or as file-less malware.

Non-College Business: A business activity that does not support the College or is not approved by the College.

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 or considerable loss of revenue (as per Douglas College Administration policy *A42 Information Security Policy*).

Personal Use: Use of College technology and/or College Resources for purposes of a personal nature, 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).

Student: A person enrolled in studies at the College in credit or non-credit courses.

D. POLICY STATEMENTS

1. Technology at Douglas College is provided to enable members of the College Community to fulfill job functions and/or 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 conduct themselves when using the College network and communication systems in a manner that is professional, courteous and respectful, consistent with College Values and policies.
   b. That they will be responsible for exercising good judgement and due care regarding the appropriate use and safekeeping of information, electronic devices and network resources in accordance with College policies and standards, and with applicable laws and regulations.
   c. That they will not share their College login credentials (login name and password) with anyone.
   d. That they will ensure that all their devices connecting to the College network and/or systems are equipped with a supported operating system and supported anti-malware, with auto-update enabled. In some situations, the College will collect the related technical data on the devices connecting to the College network.

   e. That all official communication between and among members of the College Community who have been assigned College email addresses, including active College Students, Contractors and Employees, shall be conducted through Douglas College email accounts.

3. The College has the following expectations of all Employees, including temporary and other workers as well as Contractors, 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 any personal email, non-College device or non-College cloud service or system without prior approval 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-College 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.
   h. That they will, upon request or upon leaving the employ of the College, return all College-owned devices (e.g., cell phones, laptops, tablets, wearables, web cams) to CEIT.

4. Systems access is to be granted only to authorized users following the Least Privilege Principle, on an as-needed basis, and removed in a timely manner.

5. All records created or received and all information stored by Employees in the process of conducting College business are critical assets of the College, providing evidence of its decisions, business activities and transactions; such records and information remain property of the College.

6. For the purposes of complying with legislative and policy requirements and protecting against information security concerns, the College retains the right to verify the security of devices connecting to the College network; monitor use of College equipment, systems and network traffic at any time; and access records or data when and as needed.

7. 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 prohibited.

8. 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.

9. Under no circumstances is a Student or an Employee of the College authorized to use College Resources to engage in any activity that is illegal under local, provincial, federal or international law.

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

11. Students in violation of this policy may be subject to disciplinary action under the College's policy on *Student Non-academic Misconduct*.

12. 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 that may also constitute violation of one or more of the policies listed above (see B. SCOPE) should be reported in accordance with the procedures found in the relevant policy or policies.

Standard Operating Procedure (for internal users)

- Generic Account, Generic Mailbox, or System Account Request

F. SUPPORTING FORMS, DOCUMENTS, WEBSITES, RELATED POLICIES

Administration Policies

- *Bullying and Harassment Prevention and Response*
- *College Communications*
- *Conflict of Interest*
- *Human Rights*
- *Information Security*
- *Protected Disclosure (Whistleblower)*
- *Records and Information Management*
- *Sexual Violence and Misconduct Prevention and Response*
- *Student Non-academic Misconduct*
- *Use of College Facilities*
- *Violence Prevention and Response*

Related Standards (available on DC Connect for internal users)

- 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* [SC 2010], c. 23
- *Copyright Act* [RSC 1985], c. C-42

H. RELATED COLLECTIVE AGREEMENTS

N/A