DOUGLASCOLLEGE

# ACCEPTABLE USE OF COMPUTER AND INFORMATION TECHNOLOGY POLICY

| | | |
|---|---|---|
| **Policy Name:**<br>Acceptable Use of Computer and Information Technology | **Responsible Owner:**<br>Associate Vice President, Technology and CIO | **Created:**<br>2017 Mar |
| **Policy Number:**<br>A56 | **Approval Body:**<br>SMT | **Last Reviewed/Revised:**<br>2024 Jun |
| **Category:**<br>Administration | **Replaces:**<br>N/A | **Next Review:**<br>2030 Jun |

**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 all members 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 (IT) 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 IT 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 (IT) 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 IT 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 IT in the commission of legal wrongdoing, including fraud or financial irregularity, see also Administration policies A43 *Public Interest Disclosure* (*Whistleblower)* and A76 *Fraud Prevention*.

## C. DEFINITIONS

**College Community**: All College Employees, Students and Board members, and any other person contractually obligated to comply with College policy; for the purposes of this policy, includes visiting researchers and scholars.

**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.

**Data Administrators**: Persons responsible for granting appropriate access to users.

**Employee**: A person employed by the College, including administrators, faculty members and staff, and Students when employed by the College (e.g., as Student assistants or peer tutors).

**Highly Sensitive Data (classification Level 3)**: Confidential data that if compromised can cause considerable harm or embarrassment to the College (as per 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; also refers to the team within IT Services responsible for ensuring this protection.

**Least Privilege Principle:** The principle that individuals (and systems) are to be granted only those privileges needed 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 Use:** Use of College technology and/or College Resources for purposes of a personal nature, not required for College-related activity.

**Responsible Administrator:** An executive of the College or an administrator responsible for the operations of a College department, Faculty or service area (e.g., Dean, Director, Chief Information Officer, Registrar).

**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. When Douglas College provides technology to enable members of the College Community to fulfill job functions and/or requirements of academic study, and to support a superior learning environment, 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 all applicable laws and regulations;
    c. That they will not share their College login credentials (login name and password) with anyone;
    d. That they will not use the College login credentials of another person;
    e. That they will ensure that all their devices (whether College-owned or personal) connecting to the College network and/or systems are equipped with a supported operating system and supported anti-malware, with auto-update enabled (note: in some situations, the College will collect the related technical data on the devices connecting to the College network);
    f. That they will connect personal devices only to the College's WiFi network (not to the College's wired network);

    g. That they will not attempt to tamper with or to breach the security of any computers, systems or networks, or try to disrupt, monitor or forge network or systems communications, whether those computers, systems or networks belong to the College or to other organizations; and

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

3. The College has the following expectations of all Employees, including temporary Employees and visiting researchers or scholars, with respect to their use of and access to College-related information and information technology (IT).

   a. The College expects that Employees will not

      i. Store highly sensitive information on local drives of their desktops or laptops;
      ii. Copy highly sensitive information to portable devices or portable media that do not use encryption;
      iii. Copy highly sensitive information to any personal email, non-College device or non-College cloud service or system without prior approval from both a Responsible Administrator and the IT Services Information Security team;
      iv. Use personal email to conduct business on behalf of Douglas College;
      v. Auto-forward Douglas College emails to a non-College email address;
      vi. Store any of their College login credentials in any system (e.g., email, spreadsheet) with exception of those approved by IT Services Information Security (note: use of a reputable commercial password management tool is acceptable);
      vii. Request (and IT Services will not create) generic accounts, generic mailboxes, or system accounts without appropriate approvals and without a strong business case (note: generic accounts must have an accountable account owner assigned); or
      viii. Connect devices to the College network without prior approval from IT Services (note: except where using a College device is not possible and the device meets pre-defined device security requirements, in which case connectivity of personal devices via VPN is acceptable).

   b. The College expects that Employees will

      i. Take the steps necessary to stay informed on how to be cyber-aware and cyber-safe, including by participating in relevant training;
      ii. Follow the College's Data Security Standard to safeguard sensitive information in their possession; and
      iii. 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 IT Services.

4. Data Administrators will grant systems access only to authorized users following the Least Privilege Principle, on an as-needed basis, and will remove access 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. In the event of a security breach or hardware malfunction, Information Technology (IT) Services does not guarantee that files stored on desktops or laptops will be preserved; such files may be deleted without warning if deemed necessary.

7. 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; to monitor use of College equipment, systems and network traffic at any time; and to access records or data when and as needed.

8. Personal Use of College IT 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 Non-College Business purposes is prohibited.

9. 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.

10. 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.

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

12. Students found to have violated this policy may be subject to disciplinary action under the College's policy on *Student Non-academic Misconduct*, up to and including suspension.

13. Responsible Administrators are responsible for ensuring that Employees and others under their supervision are aware of and uphold their Information Security responsibilities.

## E. PROCEDURES

Standard Operating Procedure (for internal users)

- Generic Account, Generic Mailbox, or System Account Request

**Investigating Alleged Violations of Acceptable Use of Computer and Information Technology**

1. Alleged violations of this policy that might be illegal and/or expose the College or College Resources to Significant Risk will be investigated.

2. Upon becoming aware of a potential violation of this policy, a Responsible Administrator will consult with other key College departments (i.e., Information Technology Services, Safety, Security and Risk Management, Student Affairs and/or Human Resources) to determine who will lead the investigation and who will be involved.

3. Where violations of this policy might also constitute violation of one or more other College policies, any investigation will be conducted consistent with the procedures found in the relevant policy/policies.

## F. SUPPORTING FORMS, DOCUMENTS, WEBSITES, RELATED POLICIES

Administration Policies

- *Bullying and Harassment Prevention and Response*
- *College Communications*
- *Conflict of Interest*
- *Fraud Prevention*
- *Human Rights*
- *Information Security*
- *Public Interest 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
- Data Security Standard
- How to Secure Remote Access to the College Network
- Information Technology Security Configuration and Maintenance Standards and Guidelines
- 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