



<b>Category:</b> Technology	<b>Responsible Owner:</b> VP Operations	<b>Effective Date:</b> November 14, 2024
<b>Policy/Form Number:</b> 8.1	<b>Approval Body:</b> Board of Governors	<b>Policy/Form Name:</b> Information Technology & Acceptable Use Policy

## A. POLICY

### PURPOSE/COMMITMENT:

Columbia College provides Information Technology (IT) resources to Members of the College community to support teaching, learning, and administrative goals and functions of the College.

The Director of IT Services will develop and maintain a set of IT standards to support this policy. These standards will be made available on the IT Services page of SharePoint or can be requested through the IT Department.

### SCOPE:

This policy outlines the acceptable use of Columbia College's IT resources, which include, but are not limited to equipment, software, networks, systems, data storage devices, media, facilities, and stationary and mobile devices used to access Columbia College IT resources, regardless of whether the technology or devices are personally owned, leased, or otherwise provided by the College, and used on-premises or remotely.

IT resources also include all Columbia College data, records, information, and record systems stored on or retrievable from such equipment, software, networks, systems, data storage devices, media, and facilities, or stationary and mobile devices.

### WHEN TO USE THIS POLICY:

#### Columbia College Responsibilities:

The College's obligations in relation to IT resources include ensuring compliance with applicable laws and regulatory bodies, policies and procedures, the protection of integrity and operation of its resources, and the preservation of information as necessary to protect the interests of Columbia College and to enable it to satisfy these obligations.

To ensure productive and secure operations, and to maintain optimal performance, Columbia College has adopted guidelines for the use of its technology infrastructure; all members are required to abide by these guidelines. Members should always use their best judgement when utilizing the internet and accessing the College's network resources during work hours. Use of the internet while using company hardware, whether remotely or on-premises, shall be restricted for business use.

**Privacy:** Because the primary use of Columbia College's communications and business systems is to further the institutional mission, members of the College community should not have the expectation of

privacy in their use of electronic systems, whether work-related or personal. By their nature, electronic systems may not be secure from unauthorized access, viewing, or infringement. Although the College employs technologies to secure its electronic resources and does not monitor the content on a routine basis, as a rule confidentiality of electronic data cannot be assumed. In normal circumstances, and wherever feasible, the BC Privacy Act will be adhered to. However, there may be circumstances in an emergency where it is not possible to notify or ask for approval to restore a system to its normal state, and therefore IT may be required to filter through personal data to ensure restoration is successful.

Access requested to resources not owned by the requester, must be for specific articulable reasons, must be appropriately circumscribed, and is limited to authorized personnel as approved by the Director of Human Resources. Columbia College understands that some users may have personal information and/or records on college systems, and it respects the privacy of all users as to such information insofar as possible in complying with its above-mentioned obligations. Users shall refrain from storing items of a personal nature on College resources and the College assumes no responsibility for the privacy of such information.

**Intellectual Freedom:** It is the policy of Columbia College to allow access for its community to local, national, and international sources of information and to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Nevertheless, the College reserves the right to limit or restrict the use of its information technology resources based on applicable law, institutional policies and priorities, and financial considerations.

**Standards for Accessing or Monitoring Information and Records:** Columbia College may access or monitor any/all information, records, record systems, and/or IT resources in the following circumstances:

- As necessary or appropriate to avert reasonably anticipated or already apparent threats or hazards to Columbia College information, records, or information technology resources. An example includes scanning to detect computer viruses;
- As and when required by law or to comply with legal or contractual obligations of Columbia College;
- When there is reasonable cause to believe that the employee has engaged in misconduct, has violated Columbia College policies or regulations, or may have used College resources improperly and that the information and records to be accessed or monitored are relevant to the misconduct or violation in question;
- When the College otherwise has a legitimate need to access the information, records, or information technology resources.

Reasonable efforts will be made to notify the individual of the need for access to information or records in which the individual has a substantial personal interest in information or records stored on or transmitted through the IT resources or other electronic system unless prohibited by law, inconsistent with Columbia College policy, or inconsistent with carrying out its normal operations and/or obligations.

**Preserving and Protecting Records:** In circumstances where Columbia College determines that there may be a specific risk to the integrity or security of records, data, information, or IT resources, the College may take measures to protect or preserve them. For instance, Columbia College may take a “snapshot” of a computing account to preserve its status on a given date, copy the contents of a file

folder, or restrict user access to IT resources in whole or in part. All data protected by Columbia College is stored for a minimum of 7 years.

**Remote Work and Impact to Security and Privacy:** Individuals accessing Columbia College resources, systems, and information from alternate places of work (i.e. working from home, temporary office space, or while traveling) must adhere to all Columbia College policies, procedures, laws, and regulations at all times.

Users Must:

- Access Columbia College resources, systems, and information via approved secure channels that enforce the classification of the data;
- Use only Columbia College approved software for conducting business including but not limited to email, video conferencing, and collaboration software;
- Use only Columbia College approved devices for conducting business including but not limited to laptops, computers;
- Ensure that Columbia College data and personal information or emails remain separate;
- Ensure all personal devices used to access the Internet (such as modems and WiFi) are updated with the latest operating systems, application software, and antivirus protection;
- Adhere to mandated practices to protect Columbia College information including any authentication modes and ensuring the logging off and securing devices when leaving the vicinity;
- Be alert for fraud, suspicious email, phishing, and scams that will attempt take advantage of the situation;
- Ensure printed information and other media are protected from theft and accidental disclosure and are disposed of in a manner that enforces the classification of the data (e.g. shredded);
- Backup and save Columbia College work product only to secured network drives.
- Immediately report loss or theft of a Mobile Computing Device used to conduct Columbia College business to IT Helpdesk.

In the event of a system compromise or interception at Columbia College, a proper course of action shall be implemented by the College to mitigate any form of damage, and such action shall be taken as soon as possible. Authorized personnel are to be immediately informed of such threats, whether anticipated, minor or large, and respond accordingly with the IT department. The IT Director shall lead the response to the incident.

## **Member Obligations**

**Standards of Employee Conduct for Accessing or Monitoring Records:** It is a violation of this policy for an employee to monitor information technology resources or record systems or access records beyond the standards established within this policy. It is also a violation of the policy if Columbia College has granted access to the employee (to monitor or access records or systems) and the employee has accessed or monitored records or record systems for purposes other than the purposes for which Columbia College has granted access.

## UNACCEPTABLE USES

Users may only access IT resources they are authorized for. Violations include but are not limited to:

- Failing to safeguard system integrity and accessibility;
- Sharing passwords or log-in IDs; users are responsible for all activities under their accounts. Users must notify IT if they are using a generic log-in ID and password to conduct any of their work;
- Unauthorized use of resources or another person's identity, accessing files, or processes without authorization.

IT resources must be used for their intended College business purposes and should be protected.

Violations include but are not limited to:

- Misusing software to hide personal identity to disrupt others;
- Misrepresenting identity in communications;
- Deceiving, harassing, or stalking others;
- sending threats, spam, containing malicious intent, or mass e-mails without following proper procedures or authorization;
- Unauthorized interception of communications or using resources for private advertising circumventing security measures without authorization;
- Using privileged access for non-official purposes;
- Sharing resources with unauthorized individuals;
- Retaining access after disassociating with the College.
- Using unauthorized systems to handle sensitive data;
- Creating or spreading malicious software or services;
- Preventing others from accessing an authorized service;
- Degrading performance or misusing information.

Users must comply with applicable laws and College policies. Violations include but are not limited to:

- Disregarding copyright and intellectual property laws.
- Illegally copying or distributing digital content.
- Access, sharing, storage or transmitting sensitive information without authorization or security measures.
- Using social media or third-party services to store College data without approval.

### Non-Compliance and Sanctions

Non-compliance may result in loss of access privileges and disciplinary action.

### DEFINITIONS:

**Availability** - The expectation that information is accessible by Columbia College community when needed.

**Confidentiality** - The state of keeping information and/or materials private, with only authorized individuals, processes, and systems having access to view, use, or share.

**Guidelines** - Advice on the ways to comply with policy, written for non-technical users who have multiple options for secure information handling processes.

**Integrity** - The expectation that Columbia College's information will be protected from intentional, unauthorized, or accidental changes.

**Members:** Includes employees, students, board members, consultants, temporary workers, vendors, suppliers, and any other stakeholder who requires use or access to Columbia College's technology infrastructure.

**Procedures** - Step by step instructions and implementation details for personnel to perform specific tasks in ways that ensure that the associated preventive, detective, and/or response mechanisms work as planned.

**Technology Standards** - Established requirement of technical configuration parameters and associated values to ensure that management can secure assets and comply with Columbia College policy and regulatory requirements. It is a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices.

**Responsible Owner:**

The Vice Principal Operations is the Policy Owner responsible for the oversight of this Policy. The Administration of this Policy and the development, subsequent revisions to and operationalization of any associated procedures is the responsibility of the Director of Information Technology Services.

**Category:**

8.0 Technology

**B. PROCEDURES**

**LINKS TO SUPPORTING FORMS, DOCUMENTS, WEBSITE:**

n/a

**REFERENCE TO EMPLOYMENT AGREEMENT CLAUSES:**

n/a

**REFERENCE TO BYLAWS:**

n/a

**RELATED ACTS AND REGULATIONS:**

n/a

**RELATED POLICIES:**

n/a

**C. APPROVALS:**

**WHERE APPLICABLE:**

<b>Chair, Academic Board</b> N/A	<b>Date:</b>
<b>Chair, Marketing and Recruitment Committee:</b> N/A	<b>Date:</b>
<b>Chair, Finance Committee:</b> N/A	<b>Date:</b>

**APPROVAL FOR ALL POLICIES:**

<b>Responsible Owner:</b> <u>Rose Black</u> <small>Rose Black (Nov 19, 2024 15:37 PST)</small> Rose Black, VP Operations	<b>Date:</b> 11/19/2024
<b>Principal or Designate:</b> <u>Matt Wadsworth</u> <small>Matt Wadsworth (Nov 19, 2024 15:28 PST)</small> Matt Wadsworth	<b>Date:</b> 11/19/2024
<b>Chair, Board of Governors:</b> <u>Ana Culibrk</u> <small>Ana Culibrk (Nov 19, 2024 17:54 PST)</small> Ana Culibrk	<b>Date:</b> 11/19/2024

<b>Proposed Review</b> <b>Date:</b> November 2027	<b>Dates(s) revised:</b>	<b>Replaces Policy/Form Number:</b>
--	--------------------------	-------------------------------------











# 8.1 Information Technology & Acceptable Use Policy

Final Audit Report

2024-11-20

Created:	2024-11-19
By:	Rose Black (rblack@columbiacollege.ca)
Status:	Signed
Transaction ID:	CBJCHBCAABAAGFEFPArnlJeaRjxfHouF6efscn_Mxo8C

## "8.1 Information Technology & Acceptable Use Policy" History

-  Document created by Rose Black (rblack@columbiacollege.ca)  
2024-11-19 - 11:26:10 PM GMT
-  Document emailed to Rose Black (rblack@columbiacollege.ca) for signature  
2024-11-19 - 11:26:14 PM GMT
-  Document emailed to Matt Wadsworth (mwadsworth@columbiacollege.ca) for signature  
2024-11-19 - 11:26:14 PM GMT
-  Document emailed to Ana Culibrk (aculibrk@columbiacollege.ca) for signature  
2024-11-19 - 11:26:15 PM GMT
-  Email viewed by Ana Culibrk (aculibrk@columbiacollege.ca)  
2024-11-19 - 11:26:20 PM GMT
-  Email viewed by Matt Wadsworth (mwadsworth@columbiacollege.ca)  
2024-11-19 - 11:26:23 PM GMT
-  Email viewed by Rose Black (rblack@columbiacollege.ca)  
2024-11-19 - 11:26:28 PM GMT
-  Document e-signed by Matt Wadsworth (mwadsworth@columbiacollege.ca)  
Signature Date: 2024-11-19 - 11:28:40 PM GMT - Time Source: server
-  Document e-signed by Rose Black (rblack@columbiacollege.ca)  
Signature Date: 2024-11-19 - 11:37:26 PM GMT - Time Source: server
-  Document e-signed by Ana Culibrk (aculibrk@columbiacollege.ca)  
Signature Date: 2024-11-20 - 1:54:11 AM GMT - Time Source: server

✔ Agreement completed.

2024-11-20 - 1:54:11 AM GMT