# Acceptable Use of Information Technology

| | |
|---|---|
| Policy No: | 3501 |
| Version: | 6 |
| Category: | Information Management |
| Approval Body: | Board of Governors |
| Executive Sponsor: | Chief Information Officer |
| Department Responsible: | Information Technology Services |
| Directory of Records Class: | 0650-15 |
| Approval Date: | 2020 MAY 26 |

## Policy Statement

The Institute provides information processing facilities to BCIT users to support the teaching, learning, research and administrative goals of the Institute. These resources are valuable community assets to be used and managed responsibly to ensure their integrity, security, and availability for educational and business activities.

This policy applies to all Institute information and computing, communications, and networking resources connected to Institute facilities and the users of these resources.

## Purpose of Policy

BCIT's information, network, and other information technology (IT) services are shared resources that are critical to teaching, learning, research, Institute operations, and service delivery.

The purpose of this policy is to:

- Establish responsibilities regarding acceptable use of information technology for all BCIT users
- Ensure the safe and respectful use of BCIT's information technology for all BCIT users

## Table of Contents

## Who This Policy Applies To

This policy applies to everyone who accesses BCIT's information technology assets. This includes those who use their own personal equipment to connect to Institute Information Assets.

## Related Documents and Legislation

**Legislation**
British Columbia
*College and Institute Act*, RSBC 1996, c 52
*Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165
*Personal Information Protection Act*, SBC 2003, c 63
*Human Rights Code*, RSBC 1996, c 210

Canada
*Criminal Code*, RSC 1985, c C-46
*Copyright Act*, RSC 1985, c C-43

**BCIT Policies**
1504, Standards of Conduct and Conflict of Interest
3502, Information Security
5102, Student Code of Conduct (Non Academic)
6700, Freedom of Information and Protection of Privacy
6701, Records Management
7110, Emergency Management
7170, Protection of Equipment and Property
7506, Use of Materials Protected by Copyright
7507, Harassment and Discrimination
7511, Employment and Educational Equity

**BCIT Procedures**
3502-PR1, Information Security
7100-PR1, Response to Abusive or Threatening Behaviour

## Definitions

**BCIT Internal Use:** information that is available to authorized Users and is not routinely disclosed. By default, data is BCIT Internal Use until it is assessed and otherwise classified.

**Blog:** short for “web log”, is comparable to an online journal that allows Users to post thoughts, ideas, or news items.

**Confidential Information:** information that contains sensitive Institute information and is available to authorized Users. A formal FOIPOP request is required for non-routine disclosure.

**Defamation:** a communicated statement found to be false and that causes harm to someone’s reputation.

**Directory of Records:** see Policy 6701, Records Management.

**E-communications:** the use of digital electronic technologies to communicate, including but not limited to, email systems, chat rooms, news groups, Blogs, Social Software, instant messaging and voice communication systems.

**Information Asset:** an asset that is comprised of digitized information or of equipment or systems, both fixed and/or mobile for the processing of information.

**Information Processing Facilities:** any information processing system, service, or infrastructure, or the physical locations housing them, including on-premise and cloud Services and other 3rd party providers of information processing Services. This includes computer labs, classroom technologies, computing and electronic communication devices, and Services such as modems, email, networks, and telephones.

**Instant Messaging:** a form of real time communication between two or more people based on typed text.

**Non-Institute Information:** information that is created and maintained by an individual for the purposes of that individual. Non-institute information, by definition, is not classified as Personal or Confidential by the Institute, although non-Institute information may be considered personal or confidential by the owner.

**Personal Information:** information that contains sensitive personal information and is available to authorized Users only. A formal FOIPOP request is required for non-routine disclosure.

**Services:** including but not limited to email, file storage, portals, web page hosting and other web services, and other services.

**Social Software:** software whose primary purpose is to facilitate communication between individuals and groups who share a common interest. Social Software includes, but is not limited to:

- social networking such as Instagram, Twitter and LinkedIn;
- filesharing such as Youtube, Flickr, Dropbox, Google Docs, and Box;
- instant messaging such as Messenger and Google Hangouts; and
- other publishing Services such as Blogs and Wikis, and synchronous and asynchronous chat and instant messaging tools such as Skype and on-line discussion forums.

**User:** a person who performs any action on an Information Asset.

**Wiki:** a web-based application that allows collaborative editing of its content and structure by its Users. The ease of interaction and operation makes a wiki an effective tool for mass collaborative authoring.

## Consequences of Policy Violation

The Institute reserves the right to terminate or restrict the access privileges of a User whose activities negatively affect or pose a threat to a facility, another account holder, normal operations, or the reputation of the Institute.

Following due process, the Institute may take one or more of the following actions against any User whose activities are in violation of this policy or applicable law:

- verbal or written warnings;
- restrictions or removal of access to Institute computing facilities and Services;
- legal action that could result in criminal or civil proceedings;
- for students, disciplinary action under Policy 5102, Student Code of Conduct (Non Academic); and
- for employees, disciplinary action up to and including termination.

Equipment that violates BCIT policy or negatively affects or poses a threat to a facility, normal operations, or the reputation of the Institute may be immediately disconnected, quarantined, or otherwise contained. Institute-owned equipment may also be seized.

## Duties and Responsibilities

### 1. Responsibilities by Role

***Board of Governors and BCIT Executive***

The BCIT Board of Governors and the BCIT Executive actively support and promote the acceptable use of information technology.

***Cyber Security Officer***

The Cyber Security Officer provides leadership and oversight over all aspects of cyber security, including cyber threat and risk management, developing and delivering an institutional cyber awareness program, security policies, procedures and standards formation and application. The Cyber Security Officer publishes and maintains the Information Security Standard and reviews it periodically in light of changing expectations and risks.

***BCIT Management***

Members of BCIT Management are responsible for ensuring that employees and others under their supervision are aware of their acceptable use of information technology responsibilities.

***Instructors and Teaching Faculty***

Instructors and Teaching Faculty are responsible for ensuring that students under their supervision are aware of their acceptable use of information technology responsibilities.

***IT Administrators***

IT Administrators and other privileged Users must protect the security of the information and must not abuse their elevated privileges.

***System Owners***

System Owners must ensure that all Users have been made aware of this policy and Policy 3502, Information Security, prior to granting access.

***Safety, Security and Emergency Management***

The Safety and Security and Emergency Management department is responsible for monitoring the Institute’s physical environment to ensure unacceptable behaviour is minimized.

***Risk Management***

The Enterprise Risk Management group is responsible for monitoring liability risk from Defamation and harassment.

***Users***

All Users are responsible for:

- familiarizing themselves with their responsibilities;
- complying with Policy 3502, Information Security, and other applicable Institute policies;
- complying with this Policy 3501, Acceptable Use of Information Technology; and
- promptly reporting any act that may constitute a real or suspected breach of acceptable use of information technology.

### 2. General Accountability

By using Institute Information Processing Facilities or any Information Assets, Users accept the terms of this policy and Policy 3502, Information Security.

### 3. Access

See Policy 3502, Information Security.

### 4. Copyright

All electronic data including software, music, video, and audio media that are transmitted or stored on Institute Information Processing Facilities are subject to Policy 7506, Use of Materials Protected by Copyright, and the *Copyright Act* (Canada).

Users may be required to obtain permission from the copyright owners for the digitizing, storing, sharing, and transmission of copyright-protected materials. Users must not use BCIT's Information Processing Facilities to receive, store, share, or send any unauthorized materials.

### 5. Usage Monitoring

The Institute regularly monitors its assets, and all non-Institute information transferred or stored on Institute assets may be reviewed as a result of this routine monitoring activity; Users should have no expectation of privacy regarding any Institute or non-Institute information stored on or transmitted using Institute assets.

Students using computer lab facilities during scheduled class time may be subject to monitoring at the instructor's discretion. Use of computer lab facilities at any time is subject to the routine monitoring activities.

### 6. Connecting Equipment to the BCIT Network

When connecting equipment to the BCIT network, Users are responsible for adhering to this policy and Policy 3502, Information Security. Non-compliance may result in immediate disconnection from the network.

Connection of non-Institute computer equipment to Institute Information Processing Facilities is subject to Policy 3502, Information Security. All equipment connected to the network is governed by Institute policies and may be monitored for compliance.

### 7. Use of Institute Information on Non-Institute Equipment

If an employee, student or external party stores, processes or accesses Personal, Confidential or BCIT Internal Use information on non-Institute equipment, the User and the equipment must comply with this policy, Policy 3502, Information Security, as well as the Information Security Standard 3502.

### 8. Off-Campus Use of Institute Equipment

Authorized Users of off-campus Institute-owned equipment are bound by this policy and Policy 3502, Information Security.

### 9. Personal Information Collection and Use

The collection, use, storage, and transmission of personal information are governed by Policy 6700, Freedom of Information and Protection of Privacy, and Policy 3502, Information Security.

Users are required to contact the Information Access and Privacy Office prior to collection of personal information.

### 10. Software

All software installed on Institute-owned Information Assets must be properly licensed. Users are prohibited from using Institute Information Processing Facilities or Information Assets to download, store, use, or distribute unlicensed software.

### 11. Records

When using Institute Information Assets, employees and external parties who provide Services are responsible for identifying BCIT official records and submitting those records to the designated repository according to the Directory of Records as detailed in Policy 6701, Records Management.

### 12. Personal Use

BCIT's information technology assets are intended for approved Institute purposes (including educational, academic, administrative, and research). All Users must minimize incidental personal use of Institute Information Assets. Such personal use must not increase the Institute's costs, expose the Institute to additional risk, damage the Institute's reputation, or result in personal profit.

BCIT assumes no responsibility for personal E-communications using Institute assets. Users must not misrepresent personal E-communications as official Institute E-communications.

Privately-owned software and non-Institute information is solely the responsibility of the User and will not be migrated when new computer systems are deployed. Any issues resulting from the use of privately-owned software installed on an Institute asset will result in removal of the software.

The Institute reserves the right to remove non-Institute information from storage without warning or terminate or otherwise limit the transmission of non-Institute information without warning if the storage or transmission interferes with normal operations.

### 13. Commercial Use

All use of Institute Information Assets for any business or commercial purposes must be authorized by the Institute.

### 14. Harassment

BCIT is committed to providing a learning environment where individual differences of all students and employees are valued and respected as per Policy 7507, Harassment and Discrimination. Users must not send harassing, offensive, threatening, defamatory, or obscene material by E-communications using Institute Information Assets, except in making a complaint.

### 15. Inappropriate Material

All Users are prohibited from downloading, displaying, or distributing sexually explicit or violent images, video, or audio recordings. Users shall not initiate or respond to unsolicited communication containing sexual or violent content.

This provision does not apply to the residence zone.

### 16. Responsible Use of Assets

Users must not deliberately degrade Institute Information Processing Facilities or deny service to others through any actions including excessive consumption or locking of resources including disk space, network bandwidth, and printing and processing capacity. Users have an obligation to inform system owners of their capacity requirements.

### 17. Responsible Use of Social Media

Users should refrain from including sensitive business information in the business or personal profile or posts on social media sites. Social networking sites like Facebook, Twitter and LinkedIn can be powerful tools for any business to reach potential audience but are also becoming an increasingly popular way for cyber criminals to try to get your personal or business information to hack into your personal or business enterprise systems.

### 18. Use of Email for Official Communications

Email is an official communication mechanism of the Institute. All Users must adhere to safe email practices as per Policy 3502, Information Security.

Users are responsible for ensuring that they can review official Institute emails in a timely manner. This includes account monitoring, management of storage space, and ensuring mail is flowing to any forwarded internal address.

### 19. Use of Voicemail

The BCIT voicemail system is for Institute business only. Greetings and messages must not convey or promote an employee's personal interest or private business.

Employees are responsible for managing their voicemail messages effectively. See Procedure 3502-PR1, Information Security, for details.

## Procedures Associated With This Policy

Procedure 3502-PR1, Information Security

## Forms Associated With This Policy

None

## Amendment History

| | | | Approval Date | Status |
|---|---|---|---|---|
| 1. | Creation: | Policy 3501 version 1 | 1997 Dec 01 | Replaced |
| 2. | Revision: | Policy 3501 version 2 | 2002 Jul 01 | Replaced |
| 3. | Revision: | Policy 3501 version 3 | 2003 Aug 01 | Replaced |
| 4. | Revision: | Policy 3501 version 4 | 2006 Aug 31 | Replaced |
| 5. | Revision: | Policy 3501 version 5 | 2009 May 20 | Replaced |
| 6. | Revision: | Policy 3501 version 6 | 2020 May 26 | In Force |

## Scheduled Review Date

2025 May 26