



Acceptable Use of Information Technology

Policy No.:	3501
Category:	Information Technology Services
Approving Body:	Leadership Team
Executive Division:	Learning and Technology Services
Department Responsible:	Information Technology Services
Current Approved Date:	2009 May 20

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 This 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

Policy Statement	1
Purpose of This Policy	1
Application of This Policy	2
Related Documents and Legislation	2
Definitions	3
Consequences of Policy Violation	4
Duties and Responsibilities	5
1. Responsibilities by Role	5
2. General Accountability	6
3. Access	6
4. Copyright	6
5. Usage Monitoring	6
6. Connecting Equipment to the BCIT Network	6
7. Use of Institute Information on Non-Institute Equipment	6
8. Off-Campus Use of Institute Equipment	6
9. Personal Information Collection and Use	6
10. Software	7
11. Records	7
12. Personal Use	7
13. Commercial Use	7
14. Harassment	7
15. Inappropriate Material	8
16. Responsible Use of Assets	8
17. Use of Email for Official Communications	8
18. Use of Voicemail	8
Procedures and Guidelines Associated With This Policy	8
Forms Associated With This Policy	8
Special Situations	8
Amendment History	9
Scheduled Review Date	9

Application of This Policy

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

Related Documents and Legislation

BCIT Policies:

- 1504, Standards of Conduct and Conflict of Interest
- 3502, Information Security
- 5102, Standards of Non-academic Conduct
- 6700, Freedom of Information and Protection of Privacy (FOIPOP)
- 6701, Records Management
- 7506, Copyright Compliance
- 7507, Harassment and Discrimination
- 7511, Employment and Educational Equity
- 7522, Response to Abusive or Threatening Behaviour
- 7525, Protection of Equipment, Property and Information
- 7530, Emergency Response.

Legislation applicable to this policy includes:

- *BC College and Institute Act*
- *BC Freedom of Information and Protection of Privacy (FOIPOP) Act*
- *BC Personal Information Protection (PIP) Act*
- *BC Human Rights Code*
- *The Criminal Code of Canada*
- *Canada Copyright Act.*

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 electronic technologies to communicate including email systems, chat rooms, news groups, blogs, social software, and voice communication systems.

Information Asset: an asset that is comprised of information or of equipment or systems for the processing of information.

Information Processing Facilities: any information processing system, service, or infrastructure, or the physical locations housing them. 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: include email, file storage, portals, web page hosting and other web services, and other services.

Social Software: software whose primary purpose is to facilitate communication amongst individuals and groups who share a common interest. Social software includes, but is not limited to: blogs, wikis, personal networking services (e.g., MySpace, Facebook), file sharing services (e.g., Flickr), and synchronous and asynchronous chat and instant messaging tools (e.g., Skype, on-line discussion forums, etc.).

User: a person who performs any action on an information asset.

Wiki: a web-based application that allows visitors to add, remove, and edit a public website without the need for registration. 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 the law:

- A verbal and written warning
- Restrictions or removal of access to any or all Institute computing facilities and services
- Legal action that could result in criminal or civil proceedings
- In the case of students, disciplinary action under Policy 5102, Standards of Non-academic Conduct.
- In the case of 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.

Information Security Officer

The Information Security Officer is responsible for investigating violations of this policy.

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 and Security

The Safety and Security Department is responsible for monitoring the Institute's physical environment to ensure unacceptable behaviour is minimized.

Risk Management

The 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 related Institute policies
- Complying with all the acceptable use of information technology requirements defined in this document
- Promptly reporting all acts that may constitute real or suspected breaches of acceptable use of information technology.

Duties and Responsibilities

2. General Accountability

By using Institute information processing facilities, 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, Copyright Compliance and the *Canada Copyright Act*.

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, and therefore 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 and Policy 3502, Information Security.

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 (FOIPOP) and Policy 3502, Information Security.

Duties and Responsibilities

Users are required to contact the Records Management and Privacy Office prior to collection of personal information.

10. Software

All software installed on Institute-owned assets must be properly licensed. Users are prohibited from using Institute information processing facilities 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 shall minimize incidental personal use of Institute 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 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 assets, except in making a complaint.

Duties and Responsibilities

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. Use of Email for Official Communications

Email is an official communication mechanism of the Institute. All users must adhere to Guideline 3501, Acceptable Use of Information Technology regarding the use of email.

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 address.

18. 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.

Each employee's voicemail message must follow Guideline 3501, Acceptable Use of Information Technology.

Employees are responsible for managing their voicemail messages effectively. See Guideline 3501, Acceptable Use of Information Technology for details.

Procedures and Guidelines Associated With This Policy

Guideline 3501, Acceptable Use of Information Technology.

Forms Associated With This Policy

See Guideline 3501, Acceptable Use of Information Technology.

Special Situations

None.

Amendment History

1. 1997 Dec 01
2. 2002 Jul 01
3. 2003 Aug 01
4. 2006 Aug 31
5. 2009 May 20

Scheduled Review Date

2014 May 01