Acceptable Use of Information Technology

Policy No:	3501
Version:	7
Category:	Information Management
Approval Body:	Board of Governors
Executive Sponsors:	VP Finance & Administration; VP People, Culture, & Inclusion
Department Responsible:	Cyber Security Office
Directory of Records Class:	0650-15
Approval Date:	2025 Dec 3

Policy Statement

This policy outlines the responsibilities of members of the BCIT community with respect to the responsible and acceptable use and security of BCIT IT Resources, which include technology, data, digital assets, systems, equipment and devices. It sets out requirements for the responsible, ethical, and legally compliant use of technology resources in support of BCIT operations, teaching, research, and administrative activities.

Through this Policy, BCIT seeks to foster a secure, innovative, and collaborative digital environment supporting BCIT's teaching, learning, research, and administrative goals. This Policy incorporates and adopts a risk-based and collaborative approach, encouraging both responsible technology use and the promotion of innovation to advance BCIT's academic mission. BCIT affirms its commitment to the principles of academic freedom.

Purpose of Policy

The purpose of this Policy is to establish clear expectations and requirements for the responsible and acceptable use of BCIT IT Resources by all users.

Who This Policy Applies To

This Policy applies to all individuals who use BCIT IT Resources, including staff, faculty, students, contractors, third-party contractors, researchers, and visitors. It also applies to users who use Personal Devices in connection with BCIT IT Resources.

Consequences of Policy Violation

Compliance with this Policy is mandatory for all users of BCIT's IT Resources. Users who breach this Policy or engage in Misuse will be subject to discipline, up to and inclusive of dismissal or expulsion.

BCIT reserves the right to restrict, suspend, or withdraw access to BCIT systems and services, including computing privileges and network connectivity.

Investigations of suspected Misuse and any resulting actions will follow established Institute procedures and principles of fairness and due process.

In cases where Misuse or other user equipment or activity poses an immediate security or operational risk, BCIT may take temporary measures to protect Institute systems, such as disconnecting or quarantining affected devices, until the issue is investigated and resolved.

Personal Devices connecting to BCIT networks may also be subject to reasonable security restrictions to protect Institute systems and data integrity.

Duties and Responsibilities

Role	Responsibilities
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.
Chief Information Security Officer (CISO)	The CISO provides leadership and oversight for the security of BCIT's IT systems, data, and digital assets. Their responsibilities include developing and enforcing security policies and standards, ensuring compliance with applicable regulations, and maintaining a secure and resilient infrastructure capable of detecting, preventing, and responding to cyber threats. The CISO also serves as the final authority for approving security exceptions.
BCIT Management	Members of BCIT Management are responsible for ensuring that staff and others under their supervision are aware of their responsibilities for the acceptable use of information technology.
Instructors and Teaching Faculty	Instructors and Teaching Faculty are responsible for ensuring that students under their supervision are aware of their responsibilities for the acceptable use of information technology.
IT Administrators	IT Administrators and other privileged Users must protect the security of BCIT IT Resources and must not abuse their elevated privileges.
Safety, Security and Emergency Management	The Safety and Security and Emergency Management department is responsible for monitoring BCIT's physical environment to ensure Misuse and other unacceptable behaviour is minimized.
Risk Management	The Enterprise Risk Management group is responsible for monitoring liability risk associated with the use and Misuse of BCIT IT Resources.
Users	All Users are responsible for familiarizing themselves with their responsibilities under this Policy. Users should promptly report known or suspected instances of Misuse.

1. General Accountability

All use of BCIT IT Resources is subject to compliance with this Policy. It is the responsibility of all users to ensure they are familiar with and comply with this Policy.

2. Access

BCIT's IT Resources may be accessed and used only by members of the BCIT community who are granted access privileges by BCIT. All access and use are subject to compliance with this Policy, other applicable BCIT Policies (including Policy 3502 Cyber Security) and with the applicable laws of British Columbia and Canada, including the *Criminal Code,* the *Copyright Act,* the *Human Rights Code* and the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

3. Copyright and Intellectual Property

When using BCIT IT Resources, users must comply with all applicable laws and Institute policies related to intellectual property and copyright, including BCIT Policy 7505, Use of Material Protected by Copyright, including by refraining from any acts that infringe upon copyright in relation to computer programs, data collection, work product, and any literary, dramatic, artistic and musical work.

4. Usage and Monitoring

BCIT monitors the use of its IT Resources for operational, security, and compliance purposes. Monitoring supports the protection of BCIT Data, detection and response to cyber security threats, and compliance with legal, policy and regulatory obligations. Users should understand that this monitoring and maintenance may involve access to Personal Use Records or Personal Information of users.

i. BCIT makes reasonable efforts to ensure monitoring activities are limited to what is necessary and proportionate to achieve the above purposes and are conducted in compliance with applicable legislation, including FIPPA.
ii. Users should be aware that information created, transmitted, or stored using BCIT IT Resources may be subject to access or review under circumstances such as:
    a. a suspected or confirmed security or policy incident;
    b. an investigation under Institute, legislative, policy or legal authority; or,
    c. routine system performance or security assurance activities.
iii. BCIT will not intentionally access, use, or disclose Personal Information or personal records stored on BCIT IT Resources without the user's knowledge and consent unless:
    a. authorized or required by law;
    b. where securing the user's consent would compromise the health and safety of any individual or group; or,
    c. where the information is needed for an investigation or proceeding related to a breach of law, policy, or employment duties and seeking consent would compromise the availability of required information or the investigation or proceeding.
iv. BCIT also reserves the right to access information or communications stored on BCIT IT Resources where needed to transition employment responsibilities after an employee departs from their employment or is on an extended leave.
v. Access requests involving intentional access to a user's Personal Information or Personal Use Records stored on BCIT IT Resources must be pre-authorized by the Chief Information Security Officer or their designate. Where applicable, such access will also be subject to oversight and approval from the Information Access and Privacy Office, the Human Resources department, or both, to ensure compliance with privacy, legal, and organizational requirements.
vi. BCIT recognizes the importance of privacy, academic freedom, and the confidentiality of research data. Routine monitoring of IT Resources does not involve intentional access to research data, academic work, or personal communications except as described in this Policy.

vii. Personal Devices are not subject to routine monitoring. However, network activity from Personal Devices connected to BCIT systems may be logged to detect anomalies, threats, or policy violations.
viii. All monitoring and logging activities are recorded, audited, and subject to appropriate oversight and accountability.

5. Connecting Equipment to the BCIT Network

Users are subject to the following requirements regarding devices and equipment:

i. BCIT-owned and managed equipment, including desktops, laptops, mobile devices, servers, and network-enabled systems, must comply with Policy 3502, Cyber Security and cyber security standards and requirements. These devices are centrally managed and monitored by IT Services to ensure appropriate patching, antivirus protection, and security configurations.
ii. The use of Personal Devices is permissible to enhance learning, teaching, and productivity, provided that such use does not create risks to the security, privacy, and integrity of BCIT IT Resources. BCIT reserves the right to restrict or impose conditions or security controls on the use of Personal Devices where necessary to protect BCIT IT Resources.
iii. Recognizing that academic programs and research projects often involve testing or deploying specialized technologies, faculty and research teams may connect experimental or instructional devices (including Internet of Things [“IoT”] or prototype systems) to approved lab or research networks. Such connections must be coordinated with the Cyber Security Office to ensure that security controls and network configurations protect both the research environment and the broader campus network.
iv. IoT devices (e.g., smart TVs, sensors) intended for use in buildings and in research or academic labs must be registered and approved by IT Services prior to connection. IoT devices used solely for instructional or research purposes may be connected to isolated or sandbox environments with appropriate safeguards and faculty oversight.
v. To maintain a secure and reliable technology environment, BCIT may implement reasonable measures to safeguard network performance, data integrity, and BCIT systems. These measures may include monitoring, restricting, or temporarily disconnecting devices—whether BCIT-owned, personal, or research-related—if they are determined to pose a security or operational risk to BCIT.

6. Use of BCIT Information on Non-BCIT Equipment

BCIT recognizes that users may need to access BCIT enterprise systems or communication tools from Personal Devices such as smartphones, tablets, and laptops. To protect BCIT Data while maintaining flexibility, Personal Device use is permitted under the following conditions:

i. Devices must be protected by secure login and comply with any applicable BCIT access control policies.
ii. Devices must use current operating system updates, and full-disk encryption.
iii. Users must not store or transmit sensitive Personal Information or Confidential Information on Personal Devices unless explicitly authorized by their supervisor, and in such circumstances, data must be encrypted.

iv. Personal Devices on which BCIT Confidential Information or Personal Information is stored may not be removed from Canada unless such data has been securely and permanently wiped from the device or it is otherwise permitted under this Policy.
v. BCIT files must not be synchronized to unmanaged or personal cloud storage applications.
vi. Users must not disable, bypass, or circumvent BCIT security controls, including MFA prompts or device compliance checks.
vii. BCIT Data must be securely deleted from Personal Devices once no longer needed.
viii. Any lost, stolen, or compromised Personal Devices used for BCIT purposes must be reported immediately to IT Services or the Cyber Security Office.
ix. BCIT reserves the right to restrict or revoke access if a personal device poses a security or compliance risk to BCIT systems or data.
x. Users of Personal Devices maintaining or storing BCIT records or information may be required, upon request, to provide copies of all such records to BCIT and/or to securely delete them from Personal Devices.

7. Personal Information Collection and Use

The collection, use, storage, and transmission of Personal Information is governed by Policy 6700, Freedom of Information and Protection of Privacy, and Policy 3502, Cyber Security. In accordance with FIPPA, Users are required to complete a Privacy and Security Threshold Assessment (PSTA) before implementing new initiatives, systems, programs, or projects involving the use or processing of Personal Information.

8. Responsible Use of Software and Digital Tools

BCIT supports innovation in the use of digital tools and resources. Users may explore and use digital tools to enhance academic, research, and administrative activities. Software and applications that process, store, or transmit BCIT Data must comply with BCIT's security standards and licensing requirements, and be used in accordance with Policy 3502, Cyber Security.

i. BCIT supports the responsible use of open-source, open-educational, and cloud-based tools, provided they comply with BCIT's security standards, licensing requirements, and with Policy 3502, Cyber Security and Policy 5900, Educational Technology.
ii. Users must consult IT Services or the Cyber Security Office before adopting new digital tools for teaching or research that may involve the use of BCIT enterprise systems, cloud, or data, including where they involve the collection, use or disclosure of BCIT employees' or students' Personal Information.
iii. Downloading or installing unverified or unlicensed software to IT Resources is prohibited due to potential risks to security, compliance, privacy, and data integrity.

9. Responsible Use of Hardware Assets

Users are responsible for their own use of devices and equipment in compliance with this Policy, other applicable BCIT policies, and applicable laws. In addition, where applicable users must comply with the following requirements:

i. All users are required to use BCIT-owned IT assets securely, ethically, and in alignment with authorized academic, research, administrative, or operational activities, in compliance with BCIT policies, legal requirements, and cyber security best practices.
ii. BCIT-owned equipment (e.g., laptops, mobile devices, external drives) may be used off-campus by authorized users, provided appropriate security measures are in place to protect BCIT Data and assets. Users must take reasonable steps to prevent unauthorized access, loss, theft or Misuse of devices, including secure handling, storage, and prompt reporting of any incidents of loss, theft or device compromise.
iii. BCIT equipment remains the property of BCIT and must be returned upon request or at the end of employment, contract, or academic term.
iv. Personal Devices must not be used in ways that jeopardize the security or integrity of BCIT Data or BCIT IT Resources.
v. Users are prohibited from unauthorized modification, tampering, or Misuse of BCIT owned device and equipment and other IT Resources.
vi. Users must not intentionally degrade or disrupt BCIT Information Processing Facilities, including by excessive or monopolistic use of shared resources such as disk space, network bandwidth, and processing capacity. Users are responsible for communicating their resource requirements to system owners when necessary.

10. Records

When using BCIT IT Resources, employees and external service providers are responsible for submitting relevant records to the designated BCIT records custodian in accordance with Policy 6701, Records Management. This custodian ensures that records are stored in the appropriate designated repository; that their lifecycle is managed in accordance with BCIT's Directory of Records; and all practices align with the guidelines outlined in Policy 6701, Records Management.

11. Personal Use

i. BCIT's information technology assets are intended for approved BCIT purposes, including educational, academic, administrative, and research.
ii. Users are discouraged from engaging in the use of BCIT IT Resources for personal purposes and are expected to make reasonable efforts to minimize incidental personal use of BCIT IT Resources.
iii. Any personal use of BCIT IT Resources by users must not take place during an employee's working time, and must not increase the BCIT's costs, expose BCIT to additional risk, damage BCIT's reputation, or result in personal profit.
iv. Users should also be aware that BCIT does not guarantee the security or retention of any personal content stored on BCIT IT Resources. BCIT assumes no responsibility for the retention or maintenance of such personal content, and users are responsible for maintaining their own back-up copies of such data.
v. The privacy and confidentiality of a user's personal content stored on BCIT IT Resources is also not guaranteed. BCIT IT Resources are subject to routine monitoring, access and inspection as described in this Policy, and such personal content may be accessed or accessible during such activities.

vi. Privately-owned software and non-BCIT information are 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 BCIT asset will result in removal of the software.

vii. BCIT reserves the right to manage the storage capacity and system performance of Institute-managed systems to ensure their ongoing reliability and security. Non-business or unauthorized content may be removed if it interferes with normal operations or storage availability. This provision is not intended to affect authorized academic, instructional, research, or partnership data stored on BCIT systems. Where feasible, users will be notified or consulted before any action is taken that could impact such data.

viii. BCIT email addresses and communications should not be used for conducting personal correspondence or for signing up for personal social media accounts or non-authorized services.

12. Commercial Use

BCIT technology resources are primarily intended to support educational services, academic activity, research, and administrative functions. Use of these resources to support a user's own commercial, business, external consulting, or profit-generating activities is not permitted unless such use is part of an approved academic or research initiative (including industry-sponsored projects or cooperative work experience) and has received written authorization from the Vice President with responsibility for the user's program or department.

13. Harassment and Prohibited Conduct

i. BCIT is committed to maintaining a respectful and inclusive learning and working environment where the individual differences of all students and employees are valued, consistent with Policy 7507, Prevention of Discrimination, Harassment, and Bullying.

ii. Users are prohibited from using BCIT Information Assets or electronic communication systems to transmit, display, or store any material that is harassing, offensive, threatening, defamatory, pornographic, or obscene, except where such material is required in the context of making a formal complaint under Policy 7507.

iii. Users must not engage in any behavior using BCIT IT Resources that contravenes Policy 7507, Prevention of Discrimination, Harassment, and Bullying or any related BCIT policies.

14. Inappropriate Material

Users are prohibited from downloading, displaying, or distributing sexually explicit or violent images, video, or audio recordings using BCIT IT Resources. Users must not use BCIT IT Resources to initiate or respond to unsolicited communication containing sexual or violent content (refer to BCIT Policy 7103, Sexualized Violence).

15. Responsible Use of Social Media

Users who access and use social media platforms in connection with BCIT programs or activities are expected to demonstrate good judgment and refrain from any use that is inconsistent with this Policy or other BCIT policies. Users must comply with the following:

i. Use of social media platforms on behalf of, or in connection with, BCIT programs or activities must uphold the principles of security, confidentiality, and integrity and comply with BCIT policies.
ii. Only authorized staff may manage official BCIT social media accounts, and all activities must comply with BCIT Policy 3502, as well as relevant privacy and communications policies.
iii. Users must not make personal statements on social media that directly or indirectly imply the statement are made on behalf of or have been endorsed by BCIT.
iv. Users must protect approved BCIT social media accounts using strong passwords and authentication methods, must not disclose sensitive or confidential information, and must remain vigilant against social engineering, phishing, and other cyber threats.
v. Users are expected to use social media in compliance with FIPPA and applicable intellectual property laws, including by refraining from uploading, sharing, distributing or using content or materials that infringe upon the intellectual property rights of others.

16. Use of Official Communication Tools

BCIT-approved communication platforms—including email, voice services, and collaboration tools such as Microsoft Teams ("Communication Tools")—are designated for official administrative, academic, and research-related correspondence.

i. When using the Communication Tools, Users must follow secure communication practices in alignment with BCIT Policy 3502.
ii. All users are responsible for regularly monitoring and maintaining their official BCIT email accounts and other authorized communication channels to ensure secure and timely receipt of important information. This includes managing inbox storage, maintaining access credentials, and preventing message loss due to internal forwarding, misconfiguration, or neglect.
iii. Use of Communication Tools must comply with the requirements of this Policy, including in relation to unauthorized, commercial, personal and ethical use.

17. Responsible use of Artificial Intelligence

BCIT recognizes that artificial intelligence tools, including generative AI ("AI Tools") can support research, teaching, administration, and learning activities when used responsibly, but to mitigate risk or harmful effects they must be used in ways that uphold academic integrity, ethical decision-making, privacy, and Institute values.

When used in connection with BCIT initiatives, programs, instruction, or other activities involving BCIT IT Resources, the use of AI Tools must align with BCIT's policies and security standards, and with applicable laws. In this context, all Users of AI Tools must comply with the following:

i. All proposed use of AI Tools in connection with teaching or research must be disclosed to the BCIT Information Access and Privacy Office for the completion of a Privacy and Security Threshold Assessment (PSTA).
ii. AI Tools may not be used to compile, process, assess, analyze, store or transmit BCIT Confidential Information or Personal Information unless approved in writing by BCIT. Entering or uploading student information, research data, internal documents, or any confidential content into unapproved AI Tools is strictly prohibited.
iii. Users remain responsible for all work they produce when assisted by AI Tools.

iv. All use of AI Tools must be consistent with BCIT policies and values related to equity and inclusion and must not be used to perpetrate bias or discrimination.
v. Users must review all AI-generated content for accuracy, bias, copyright compliance, and appropriateness before use or dissemination.

18. Use of BCIT-Issued Devices During International Travel

Removing BCIT Data or BCIT IT Resources for the purposes of work-related or personal travel creates privacy and security risks. Users must comply with guidance issued by IT from time to time regarding the access to or use of IT Resources in connection with out-of-country travel.

Forms Associated with This Policy

None

Amendment History

			Approval Date	Status
1.	Created:	Policy 3501 version 1	1997 Dec 01	Replaced
2.	Revised:	Policy 3501 version 2	2002 Jul 01	Replaced
3.	Revised:	Policy 3501 version 3	2003 Aug 01	Replaced
4.	Revised:	Policy 3501 version 4	2006 Aug 31	Replaced
5.	Revised:	Policy 3501 version 5	2009 May 20	Replaced
6.	Revised:	Policy 3501 version 6	2020 May 26	Replaced
7.	Revised:	Policy 3501 version 7	2025 Dec 03	In Force

Scheduled Review Date

2030 December 3. This policy must be reviewed no later than five years from approval. However, it may be updated as needed to address emerging threats, changes in technology, or regulatory requirements.

Related Documents and Legislation

Law/Regulatory/Policies	Document Name
Legislation	British Columbia *College and Institute Act*, RSBC 1996, c 52 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165 [FIPPA] *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	1100, Public Interest Disclosure & Protection 1200, Fraud 1300, Enterprise Risk Management 1500, Code of Conduct 3502, Information Security

	5102, Student Code of Conduct (Non-Academic) 5900, Education Technology 6700, Freedom of Information and Protection of Privacy 6701, Records Management 7100, Safety and Security 7103, Sexualized Violence 7110, Emergency Management 7170, Protection of Equipment and Property 7506, Use of Materials Protected by Copyright 7507, Prevention of Discrimination, Harassment & Bullying 7511, Employment and Educational Equity

Definitions

Term	Definition
Access	The authorized ability to use, read, enter, modify, communicate with, or otherwise interact with information, systems, applications, networks, or data. Access may be physical (entry to secure facilities or server rooms) or logical (digital permissions granted through authentication and authorization).
AI	Artificial Intelligence
BCIT Data	Means Personal Information and Confidential Information.
BCIT IT Resources	Any device, system, software, application, data, or network component that is owned, leased, or managed by BCIT, or otherwise used to store, process, transmit, or secure Institute information. IT Assets include computing devices, servers, mobile equipment, cloud and network services, and digital information repositories that support BCIT's teaching, learning, research, and administrative operations.
Digital Tool	Any application, platform, website, software, or online service—whether locally installed, cloud-based, or web-hosted—enabling users to create, access, process, communicate, or share digital information. Digital tools include, but are not limited to, learning management systems, collaboration platforms, productivity applications, research or data analysis tools, generative AI platforms, and open-source or commercial software used in teaching, learning, research, and administration.
Confidential Information	Means information about BCIT programs, systems, processes, plans, research, trade secrets, and proprietary knowledge and materials that is not generally known, used, or available.
Information Processing Facilities	Any information processing system, service, or infrastructure, or the physical locations housing them, including on-premise and

Term	Definition
	cloud Services and other third-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.
FIPPA	Means the BC *Freedom of Information and Protection of Privacy Act,* including all regulations and amendments.
Instant Messaging	A form of real time communication between two or more people based on typed text.
Misuse	Means any use of BC IT Resources in violation of this Policy, FIPPA or other applicable laws.
Monitoring	The collection and review of technical system data for the purpose of ensuring operational integrity, cyber security, and legal compliance. Monitoring does not imply unrestricted access to user content.
Non-BCIT Information	Means recorded information in the custody and control of BCIT that has not been collected, used, stored or disposed of for the purpose of BCIT business.
Personal Devices	Means user-owned devices, including laptops, tablets and other digital devices and equipment.
Personal Information	Means any recorded information about an identifiable individual, including without limitation, students, staff, researchers, research subjects, volunteers, and visitors, other than business contact information.
Personal Use Records	Means records that do not relate to BCIT business, programs or activities that a user creates, stores or maintains through IT Resources.
Privacy Risk Assessment (PIA)	Means an assessment conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of the *Freedom of Information and Protection of Privacy Act*.
Privacy and Security Threshold Assessment (PSTA)	Means an assessment conducted by BCIT to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of the *Freedom of Information and Protection of Privacy Act.*
Services	Includes but is not limited to email, file storage, portals, web page hosting and other web services, and other services.
Social Media Software	Any online application, platform, or tool that enables users to create and share content or participate in social networking. This includes, but is not limited to, platforms such as Facebook, X (formerly Twitter), Instagram, LinkedIn, and TikTok, as well as any internal social or collaborative tools.
User	A person who performs any action on an Information Asset.