SAIT

AD.2.15.1

ACCEPTABLE USE OF COMPUTING, INFORMATION AND TECHNOLOGY RESOURCES

Section**:** Administration (AD)
Subject**:** Institute and Non-Institute Services

Legislation: *Freedom of Information and Protection of Privacy Act* (RSA 2000 cF-25); *Health Information Act* (RSA 2000 cH-5).
Effective**:** November 21, 2019
Revision**:** September 18, 2023; June 5, 2024

APPROVED: ______________________________
President and CEO

POLICY

The policy of the Board of Governors is that members of the SAIT community will use SAIT's computing, information and technology resources only for the purposes for which they are intended, and shall be held accountable for their misuse of those resources.

PROCEDURE

DEFINITIONS

Computing, information and technology resources All hardware, software, data, network access, and computing services provided and managed by SAIT. This includes but is not limited to computer systems, mobile devices, network devices, peripherals/printers, software applications, databases, and electronic information that are owned, managed and/or operated by SAIT, as well as the use of external services such as cloud computing and storage services.

Personal information Recorded information about an identifiable individual and includes, but is not limited to, name, residential address and phone number, personal email address, sex (sex assigned at birth), gender identity, title, pronouns, sexual orientation, religious affiliation, Indigeneity, ethnicity, disability status,

The official controlled version of this document is held in the Board of Governors Office.

languages spoken, immigration status, identification number, education and employment history, health information including documentation of approved accommodations for physical or mental disability, an individual's personal views or opinions and information about an individual's financial matters.

SAIT community SAIT's governors, employees, students, alumni, contractors, consultants, agents, and volunteers.

GOVERNING PRINCIPLES

1. In order to create and foster a positive academic environment, maintain business continuity and enhance SAIT's reputation, it is critical that SAIT protects the confidentiality, integrity and availability of its computing, information and technology resources.

2. Members of the SAIT community are governed by this procedure and by applicable provincial and federal legislation in their use of SAIT's computing, information and technology resources.

3. SAIT strives to foster and maintain an intellectual environment in which members of the SAIT community can access and create information, and can collaborate with colleagues and peers. Use of SAIT's computing, information, and technology resources should never impede SAIT's goal of a being a positive teaching, learning, and research environment. This procedure helps SAIT to achieve these goals.

4. This procedure applies to SAIT employees who use their personal electronic devices for work-related purposes.

PROCEDURE

A. Personal Use

1. SAIT permits members of the SAIT community to make personal use of SAIT computing resources, provided they limit such use so that they do not consume an unreasonable amount of these resources and they do not interfere unreasonably with the activity of other users, with SAIT's business or systems. Accordingly, SAIT may

require users of its computing, information and technology resources to limit or refrain from specific uses.

2. SAIT will assess the reasonableness of any particular use in the context of all relevant circumstances.

3. SAIT is not responsible or liable for content that members of the SAIT community personally choose, at their sole discretion, to download, send or store on SAIT's information systems, or for any disclosure, use or loss of such content. Any such content that is downloaded, sent to or stored by a SAIT community member is at their sole and exclusive risk.

B. Commercial Use

1. Use of SAIT's computing, information and technology resources for commercial purposes is governed by SAIT's policies and procedures relating to conflict of interest.

C. Copyright and Intellectual Property

1. Users of SAIT's computing, information and technology resources must uphold procedure AC.2.11.1 Intellectual Property, procedure AC.2.12.1 Copyright of External Materials, and Canadian law relating to copyright and to intellectual property, including but not limited to trademarks, trade names, logos, etc.

D. Illegal or Malicious Activity

1. Users of SAIT's computing, information and technology resources may not use SAIT resources to breach or to attempt to breach federal, provincial or municipal law. Examples of illegal or malicious activity include but are not limited to:

    a) Uttering threats (by computer, email or telephone).

    b) Pornography.

    c) Gambling, betting, or pyramid schemes.

    d) Cyberbullying.

    e) Hacking into the computers of other members of the SAIT community.

f) Launching cyberattacks.

g) Theft.

h) Inappropriate use of SAIT's 3D computer printing resources.

2. SAIT will report suspected violations of federal, provincial or municipal law to the appropriate law enforcement agencies.

3. A member of the SAIT community found to have breached federal, provincial or municipal law in the use of SAIT's computing, information and technology resources may be subject to the sanctions and discipline set out in procedure AC.3.4.4 Student Non-Academic Conduct and/or HR.4.1.1 Corrective Action.

E. Credentials and Identity

1. SAIT will provide each user of its computing, information and technology resources with one or more sets of identifying credentials intended for that individual's exclusive use.

2. An individual granted authorization to use an electronic identity must make all reasonable efforts to keep such information private and secure, and may not:

   a) Share credentials (username/password) with anyone other than the designated owner of those credentials.

   b) Log into a resource with a credential other than one that the individual has been assigned or authorized to use.

   c) Use any credentials to access information or material that the individual is not authorized to view.

3. Credentials for shared/functional accounts should only be shared with individuals who have a need to access the account, and passwords should be changed whenever changes are made to this access.

4. For further information on passwords, refer to procedure AD.2.10.1 Password Guidance.

F. Confidentiality and Integrity of Data

1. Users of SAIT's computing, information and technology resources who are given access to personal information, sensitive and/or confidential information, records and/or data must comply with procedure AD.1.1.1 Personal Information – General Guidelines Procedure, procedure AD.3.2.1 Records Management and procedure AD.3.3.1 Data Governance in their access and use of that information, records and data.

2. Data will be managed as a business-critical resource by following data management best practices and principles that safeguard the data's integrity, security, ownership and access. See procedure AD.3.3.1 Data Governance for further information.

G. Ethics/Respect

1. Users of SAIT's computing, information and technology resources are expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.

2. Users are required to engage in ethical behaviours, including:

   a) Honesty (both academic and in business activities).

   b) Acceptable language or discourse.

   c) Restraint in the consumption of shared resources.

   d) Respect for other individual's rights of freedom from harassment in forms such as intimidating, disrespectful or obscene messages, jokes or images.

H. Systems Administration

1. SAIT has the right to access, monitor and record stored and/or in-transit SAIT data and the usage of computing, information and technology resources when there is:

   a) Suspected or alleged impropriety (including a data breach event).

   b) A business need for access when an employee is absent.

   c) A request arising in relation to legislation.

d) As otherwise required by law.

2. SAIT has the right to use information gained in this way in disciplinary actions as per procedures AC.3.4.3 Student Academic Conduct, AC.3.4.4 Student Non-Academic Conduct and/or HR.4.4.1 Corrective Action, and to provide such information to appropriate internal and external investigative and/or law enforcement authorities.

I. Unacceptable Use

1. Users shall not use any computing, information and technology resources to:

a) Cause harm or disruption to SAIT computing, information and technology resources.

b) Alter or modify any operating system, software, hardware, or system configurations that compromise security or safety.

c) Initiate actions that defeat or circumvent SAIT security measures and restrictions.

d) Execute any form of non-approved network monitoring that will intercept data, with the exception of troubleshooting or implementing SAIT technology and information systems.

e) Create or introduce malware harmful to the operation of any SAIT computing, information and technology resources.

f) Gain unauthorized access to systems.

g) Interfere with, or disable, another SAIT user's access or an administrator's access.

h) Distribute to internal or external parties any product or information asset without appropriate authorization.

i) Open email attachments from unknown sources or interact with links to unknown websites in emails.

j) Forward phishing email tests within the organization, with the exception of reporting to the Service Desk or Cybersecurity.

The official controlled version of this document is held in the Board of Governors Office.

k) Store passwords on computer systems or files. Users are required to use only approved password managers for the safe storage of passwords utilized for access to SAIT's computing, information and technology resources.

2. Users must not leave their computing devices unlocked when unattended.

J. Compliance

1. Any breach of this procedure may be dealt with as per procedure AC.3.4.4 Student Non-Academic Conduct, procedure HR.4.4.1 Corrective Action, and/or any applicable collective agreement or terms of employment.

K. Obligation to Report

1. Users of SAIT's computer, information and technology resources shall report any violations of this procedure to the Information Technology Services department, through the Service Desk.

2. An individual who suspects that there has been unauthorized access to that individual's account or that abuse of other computing, information and technology resources has occurred must promptly bring the situation to the attention of the administrators of the system or the Service Desk.

3. Users must immediately report lost or stolen SAIT technology resources to the Service Desk.

L. Unauthorized Network Devices

1. Members of the SAIT community shall not connect any network devices or systems (including but not limited to switches, routers, wireless access points, VPNs, and firewalls) to SAIT's network without Information Technology Services' prior approval.

POLICY/PROCEDURE REFERENCE

AD.2.15	Acceptable Use of Computing, Information and Technology Resources policy
AD.2.15.2	Student Identity Digital Management procedure
AD.2.15.3	Use of Artificial Intelligence Technologies at SAIT procedure

The official controlled version of this document is held in the Board of Governors Office.