

---

## Information Technology Usage Policy - Staff

### 1.0 Purpose

To provide guidance to BKI staff on acceptable use of Information technology resources, including Artificial Intelligence (AI) tools provided by BKI.

### 2.0 Scope

The policy applies to all Staff (academic or professional) of BKI.

### 3.0 References

Privacy and Data Protection Act 2014 (Vic)

Privacy Act 1988 (Cth)

Copyright Act 1968 (Cth)

Copyright Amendment (Digital Agenda) Act 2000 (Cth)

Australia's Artificial Intelligence Ethics Framework 2019

### 4.0 Policy Statement

BKI provides access to Information Technology (IT) systems, software resources, and the latest AI-enabled tools BKI **Staff (academic or professional)**. This access aims to support and enhance the work and professional development of staff.

**Staff** are encouraged to use these resources:

- To improve their efficiency and effectiveness in their roles.
- To facilitate communication and collaboration with colleagues and students.
- To enhance their professional development.

BKI staff are advised that with the opportunity to use BKI's IT and AI resources comes the responsibility to behave legally, ethically, morally, and according to the standards of behaviour outlined in the BKI Code of Conduct Policy.

This revision emphasises that BKI's resources are available to both students and staff. It clarifies how the resources can benefit staff and highlights the shared responsibility for ethical and appropriate use.

#### 4.1 Acceptable Usage

Each individual must respect the right of others to work and/or study in an environment which is free from harassment and intimidation when using BKI's IT resources. Acceptable uses of BKI's IT resources are activities which directed at proper learning and teaching.

BKI staff are encouraged to develop usage which meets their work-related needs, and which take advantage of BKI's IT functions such as portals, email, instant messaging, web access, conferencing/collaboration, bulletin boards, databases and access to software.

---

## Information Technology Usage Policy - Staff

Staff are granted access to BKI's technology resources to perform their job duties effectively. Acceptable use includes:

- Staff should be aware that transferring excessively larger files can have an adverse effect on network resources and negatively affect BKI operations and other BAU activities. This practice is strongly discouraged.
- Staff should use BKI provided technology resources for work-related purposes only. Personal use should be kept to a minimum and should not interfere with job responsibilities.
- Staff members are expected to use technology resources in a manner consistent with the educational mission and values of the institute.
- Staff members are responsible for safeguarding institute-owned technology resources against unauthorised access, loss, theft, or damage. Any suspected security breaches must be reported to the IT department immediately.
- Staff members must adhere to all security protocols, including the use of strong passwords, regular system updates, and not sharing confidential information over insecure channels.
- Internet access provided by the institute is to be used for work-related research and communication to perform their respective work effectively.
- Email, conferencing/collaboration tools, mobile phone and other communication accounts provided by the institute are to be used for professional communication only. Confidential information should not be shared over insecure mode of communication / medium / channels.
- Institute-provided software and data should only be used for authorised purposes.
- Unauthorised copying, distribution, or use of software or data is strictly prohibited.
- Staff members are expected to communicate respectfully and professionally in all electronic communications, including emails, instant messages, and social media interactions. Additionally, harassment, discrimination, or any form of inappropriate behaviour is strictly prohibited.

Furthermore, with the introduction of AI resources and tools, the following forms part of the acceptable usage of BKI's technology resources by Staff:

1. Staff members are expected to use AI tools and services in a responsible, ethical, and legal manner, ensuring that they comply with all applicable laws, regulations, and Institute policies.
2. Staff members should be aware of the limitations and potential biases of AI tools and services and should not rely solely on AI-generated outputs for decision-making.
3. Staff members must ensure that any AI-generated content or recommendations are appropriately reviewed and verified before being used in an educational setting.
4. Staff members are responsible for maintaining the privacy and security of any personal information collected, stored, or processed by AI tools and services, in accordance with the Institute's Privacy Policy and other relevant policies.
5. Staff members should consider the potential ethical implications of using AI tools and services, including issues related to fairness, transparency, and accountability.
6. Staff members should report any concerns or potential breaches of this Policy to their supervisor or the appropriate Institute authority.

---

## Information Technology Usage Policy - Staff

### 4.2 Unacceptable use of network and physical devices

Staff must not:

- use BKI's IT resources to download, display, share or print offensive material, including material that is sexist, sexually explicit, pornographic or racist.
- knowingly receive and utilise material via email or through the Internet that is offensive, including material that is sexist, sexually explicit, pornographic or racist.
- use BKI's IT resources to threaten, harass, defame or offend others, or to discriminate against others or to use BKI's IT resources in a vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or other offensive manner.
- attempt to transfer, store or print files, material or messages that violate antidiscrimination legislation, copyright law or BKI policies and procedures, or display or transfer offensive materials via BKI's IT resources.
- violate the rights to privacy of students or BKI's employees, contractors, volunteers or guests including attempts to access another person's account, private files, or email without the permission of the owner.
- attempt to write, produce, copy or attempt in any way to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any computer.
- attempt to alter system software, firmware or hardware configurations or corrupt, damage or destroy data.
- use BKI's IT resources for any non-BKI related commercial purpose.
- misuse IT equipment; care must be exercised at all times when using IT equipment, staff will be held responsible for the cost of repair if damage is caused through misuse or negligence.
- damage IT equipment. Any damage must be reported to BKI staff immediately upon discovery.
- tamper with or move IT assets without authorisation.
- record and transmit images, voice, video and files without permission of the person and where the person is a child or young person under the age of 18, without permission from a parent or carer as well.
- utilise staff email to spam or otherwise create or submit unwanted emails to any other internal or external users.

Staff must not use AI resources and tools for the following:

- **Personal or Inappropriate Purposes:** AI tools and services should not be used for personal gain or inappropriate purposes, such as harassing, discriminating, or spreading misinformation within the BKI community.
- **Privacy Violations:** Staff members should not use AI tools and services to collect, store, or process personal information of students, colleagues, or other stakeholders without proper consent or in violation of data protection regulations and BKI policies.
- **Lack of Transparency:** Staff members should not conceal their use of AI tools and services, particularly when making decisions that affect students or colleagues. Deliberately hiding the involvement of AI in decision-making processes can erode trust and lead to ethical concerns.
- **Unethical Behaviour:** Staff members should not use AI tools and services in ways that promote or facilitate unethical behaviour, including discrimination, bias, or unfair treatment within the BKI community.

## Information Technology Usage Policy - Staff

- **Misrepresentation of AI-generated Outputs:** Staff members should not present AI-generated outputs as human-produced content or manipulate AI-generated outputs in ways that could deceive or mislead students, colleagues, or other stakeholders.
- **Ignoring AI Limitations:** Staff members should not blindly rely on AI-generated outputs without considering the limitations and potential biases of the AI tools and services being used, especially when making decisions related to student learning and assessment.
- **Neglecting Security:** Staff members should not disregard security best practices when using AI tools and services, which could lead to unauthorised access, data breaches, or other potential threats to the BKI community.
- **Failure to Report Misuse:** Staff members should not ignore or cover up instances of misuse, abuse, or violation of AI policies by themselves or others within the BKI community.

### 4.3 Reporting receipt of offensive material

Staff (academic or professional) who receive unsolicited offensive material from an unknown external source or a known source within BKI must report it immediately to the relevant supervisor, manager or department head, who will determine the further actions required. Staff must not print or forward the offensive material. In case of incidents where offensive material involves children or young people under or appearing to be under the age of 18 refer to the Child Safety Procedure for reporting requirements.

### 4.4 Breach of this Policy

Any employee that becomes aware of an actual or possible breach of this policy should immediately report the matter to the ICT Support Centre. Any instances of unauthorised use will be investigated and reported. Users may be asked to cooperate with any investigation into a security breach or improper use.

Users may be held personally liable for damages or costs incurred as a result of their actions. Any BKI staff found to be in breach of this Policy may have disciplinary action initiated against them, in accordance with the BKI's Code of Conduct Policy.

## 5.0 Roles and Responsibilities

Role	Responsibilities
Staff	Staff members are responsible for safeguarding institute-owned IT resources against unauthorised access, loss, theft, or damage. Any suspected security breaches must be reported to the IT department immediately.
Staff	<ul style="list-style-type: none"> <li>• Using strong passwords and keeping them confidential.</li> <li>• Exercising caution when opening emails or attachments from unknown senders.</li> <li>• Updating windows and backing up important data regularly.</li> </ul>

## Information Technology Usage Policy - Staff

CIO	Investigate breaches of proper use of BKI Systems and AI resources
Head of the SARC	Evaluate and approve AI tools before deployment, ensuring alignment with this policy and ethical guidelines.

### 6.0 Definitions

Word/Term	Definition
BKI	Bendigo Kangan Institute
Data	Includes all information captured, used, exchanged and stored electronically.
Hardware	Any computer, portable electronic device (including mobile phones and tablets), communication, printing or storage device, media and associated equipment in use with BKI IT systems.
Software	Any operating system, program, application or instruction routine in use or stored on BKI IT systems
IT Resources	Includes all computers and computing devices (both the wired and wireless local and wide area networks) as well as any software and other IT related services provided by BKI for student/staff use.
Artificial Intelligence	Artificial intelligence (AI) refers to computer systems capable of performing complex tasks that historically only a human could do, such as reasoning, making decisions, or solving problems.

### 7.0 Supporting Policies and Forms

Policy or Form name
BKI Code of Conduct Policy – Staff
BKI Child Safety Policy and Procedures
Feedback Policy (Compliments and Complaints) and Feedback Procedure (Compliments and Complaints)

### 8.0 Version Control and Change History

Ver.	Issue Date	Document Custodian	Description of Change	Approved By
1.0	26/04/2021	CIO	New Policy created for students	Head of Technology Strategy, Architecture, Risk and Compliance
2.0	28/03/2024	CIO	Addendum – AI Resources and tools acceptable usage and other terms and conditions	Head of Technology Strategy, Architecture, Risk and Compliance

**Information Technology Usage Policy - Staff**

3.0	[ ]/[ ]/2024	CIO	Addendum – Staff AI Resources and tools acceptable usage and other terms and conditions	Head of Technology Strategy, Architecture, Risk and Compliance
-----	--------------	-----	---	--

**9.0 Document Owner and Approval Body**

Document Custodian	Approval Authority	Approval Date	Scheduled Review Date
Head of Technology Strategy, Architecture, Risk and Compliance	Chief Information Officer	09/09/2024	09/09/2026