Information Technology Usage Policy

1.0 Purpose

To provide guidance to Bendigo Kangan Institute (BKI or the Institute) employees, contractors, service providers, and volunteers on acceptable use of Information technology at work.

2.0 Scope

This policy applies to employees, contractors, service providers, and volunteers, regardless of the manner of employment.

3.0 Legislative Context

Privacy and Data Protection Act 2014 (Vic)

Privacy Act 1988 (Cth)

Copyright Act 1968 (Cth)

Copyright Amendment (Digital Agenda) Act 2000 (Cth)

Financial Management Act 1994 (Vic)

Child Wellbeing and Safety Act 2005 (Child Safe Standards)

4.0 Policy Statement

4. 1 Acceptable Usage

The use of BKI information and communication technology resources and equipment is to be done so in accordance with business and regulatory requirements. This policy sets out the direction, principles and business rules that govern all use of those resources. Devices not owned by BKI but authorised for use on BKI systems (BYOD), are also subject to this policy.

Reasonable personal use of ICT resources, including email, SMS, is permitted. However, users should note that email accounts, computers and network storage are intended primarily for work use. All information in these systems is accessible to BKI for review, audit, and archiving purposes and all materials held on BKI systems or transmitted through BKI accounts may, with approval of the Executive responsible for the portfolio, be made accessible to other BKI employees. Personal information or communications which you consider confidential and which you do not wish to be disclosed, should not be sent, or stored on BKI IT systems.

4.2 Unacceptable Usage

- Illegal or criminal purposes.
- To threaten, harass, offend, annoy, slander, bully, intimidate, libel, or interfere with the work of any person.
- To play games or streamed content during working hours, unless authorised for work-related purposes.
- Install software without prior authorisation by the relevant System Administrator.
- To transmit or broadcast, within or outside the organisation, spam, chain letters, junk mail, unsolicited commercial messages or content, political material or opinion, unsolicited

religious messages or content, or to conduct surveys/questionnaires not expressly authorised by BKI.

- For gambling.
- Transmit or download, invite, or send messages or material that is pornographic, or sexual, or child abuse material, constitutes cyber abuse or of an offensive nature.
- To substantially conduct or facilitate a private business. As an example, checking an on-line share portfolio does not constitute substantially conducting a business, whereas regular buying and selling on eBay would.

4.3 Students Under 18 Considerations

- 1:1 contact with students under the age of 18 using IT equipment including phones, computers, online classes, forums, and meetings is not advised without prior student and parent/carer informed consent.
- Whereby 1:1 contact occurs, for example, in the counselling space, and confidentiality a requirement this is documented, approved, and overseen by the appropriate manager.
- BKI approved email addresses are to be used for both workers and students.
- Student emails consist of their ID number and use of student names in email addresses is avoided.
- When sending group emails to students and families, it is advised to use the blind CC option so that other students and families do not inadvertently have access to the private information of others.
- Parent/carer of students under 18 are provided a copy of the Information Technology Usage Policy (Student), and the details of the student email used by TAFE.
- For virtual classrooms and assessments:
    - Students enrolled prior to June 2022 the Digital Delivery Consent for Students under the age of 18 is signed by parent/carer at enrolment. This is the responsibility of the program.
    - Student enrolments post June 2022 the enrolment form itself accessible via the Registrar and Student Administration share-point page here covers parent/carer consent for students under the age of 18 to participate in virtual classrooms and assessments, i.e., video submissions.
- For VETDSS students the schools provide consent on behalf of parent/carers for these students to engage in virtual classrooms or submit video assessments.

Note: If consent not obtained discuss alternatives with the student and parent/carer, or school for VETDSS.

4.4 Other Responsibilities

- Keep equipment secure when it is provided to you.
- Keep information that is stored on the machine or network secure.
- Notify ICT immediately where a security breach occurs.

Information Technology Usage Policy

- Note that if you store your own non-work-related information on the system, BKI is not responsible for its security.
- Not send BKI confidential material or information to unauthorised persons inside or outside BKI.
- Ensure that all use of technology is consistent with the BKI Employee Code of Conduct.

4.5 Breach of this Policy

Actual or possible breaches of this policy should immediately be reported to the Group Manager ICT. Instances of unauthorised use will be investigated and reported. Users must cooperate with any investigation into a security breach or improper use.

Users may be held personally liable for damages or costs incurred because of their actions.

Established breaches of this Policy may have disciplinary action initiated in accordance with the Employee Code of Conduct and Employee Disciplinary Procedure

4.6 IT Security

IT security threats aim at corrupting or stealing data to disrupt an organisations systems or data privacy. Threats include spam, scams such as phishing, which can be targeted via email, SMS or phone calls.

BKI use several protections such as password protected access to computers, access to intranet, emails, and BKI applications so as at minimum a twostep authentication process to access personal or sensitive information. Work mobiles are to be set with password and fingerprint access with automated locking when not in use.

Third party applications such as Microsoft Teams and Air Table are not to be used to store sensitive information that could identify persons, such as student identifiable information, or personal email accounts.

5.0 Roles and Responsibilities

Role	Responsibility
Group Manager ICT	Establish and maintain a system of management of the ICT systems and assets. Liaise with relevant people leaders and Head of People Operations when a breach reported and established.
ICT Team Members	Support the use of ICT assets.
Head of People Operations	Ensure processes in place to manage and investigate breaches to this or other relevant policies, or codes of conduct.

Information Technology Usage Policy

People Leaders	Ensure breaches of this policy related to persons within remit are managed in accordance with relevant codes of conduct and disciplinary procedures.
Employees, contractors, service providers, volunteers	Use ICT assets and systems in an appropriate manner, in accordance with this policy.

6.0 Definitions

Word/Term	Definition
BYOD	Bring Your Own Device, a portable electronic device personally owned such as a laptop, smart phone, or tablet device.
Child Abuse Material	Depicts or describes, a person who is, or who appears or is implied to be, a child, (as person under the age of 18 years) as a victim of torture, cruelty or physical abuse (whether or not the torture, cruelty or abuse is sexual); or as a victim of sexual abuse; a sexual pose or sexual activity; or in the presence of another person who is engaged in, or apparently engaged in, a sexual pose or sexual activity; or the appears to show the privates parts of a person who is, or who appears or is implied to be, a child.
Cyber Abuse	Is when the internet is used to send, post, or share content that is harmful to the physical or mental health of someone.
Data	Includes all information captured, used, exchanged, and stored electronically.
Employees, contractors, service providers, volunteers	Includes all workers whether paid or unpaid, short-term contractors, interns, persons on placement or work experience for example.
Hardware	Any computer, portable electronic device, communication, printing or storage device, media, and associated equipment in use with BKI IT systems.
ICT	Information Communication Technology
IT	Information Technology
Group Manager ICT	BKI's IT Manager.
Phishing	A type of scam, involving sending communication (usually email, can also be phone call or SMS) disguised as being from a trusted sender to steal confidential information.
Scam	A deceptive scheme or trick used to cheat someone out of something, especially money. Example: Banks will never call you asking for your credit card number or social security number over the phone.
SMS	Short Message Service, commonly known as texting.

Information Technology Usage Policy

Software	Any operating system, program, application, or instruction routine in use or stored on BKI IT systems.
Spam	Unauthorised and/or unsolicited electronic mass messages.

7.0 Supporting Policy Document and Forms

Document Name
Employee Code of Conduct
Employee Disciplinary Procedure (Policy in draft)
Positive Workplace Behaviours Policy
Human Rights Policy (in Draft)
Child Safety Policy and Procedure
Information Technology Usage Policy (Student)
Digital Delivery Consent for Students under the age of 18
BT and KI interactive & printable Enrolment forms here

7.0 Version Control and Change History

Ver.	Approved By	Approval Date	Issue Date	Description of Change	Next Scheduled Review Date	Document Owner
1.0	Board	27/10/2014	04/12/2014	The content of this policy originated from Bendigo TAFE POL 303 Information Technology Usage Policy.	31/12/2015	Executive Director Learning Experience
2.0	N/A		02/03/2015	Editorial change: Removal of logos from template	31/12/2015	Executive Director Learning Experience
2.1	CEO	15/06/2016	15/06/2016	Scheduled review	15/06/2018	COO
2.2	CEO	24/08/2017	30/08/2017	Clarify privacy	30/08/2019	COO

Information Technology Usage Policy

Ver.	Issue Date	Document Custodian	Description of Change	Approval Authority
2.3	30 Jun 2022	Cyber Security and Compliance Manager	Updates to reflect Child Safe Standards	Head of Legal, Governance, Risk and Compliance

9.0 Document Owner and Approval Body

Document Custodian	Approval Authority	Approval Date	Issue Date	Scheduled Review Date
Cyber Security and Compliance Manager	Head of Legal, Governance, Risk and Compliance	29 Jun 2022	30 Jun 2022	30 Jun 2024