Apprenticeships Are Us

ACCEPTABLE USE OF ELECTRONIC MEDIA POLICY

TABLE OF CONTENTS

INTRODUCTION

Apprenticeships Are Us Ltd (ARU) recognises that workers may need access to Electronic Media Systems and Associated Tools to fulfill their roles. This policy is established in alignment with the *Fair Work Act 2009 (Cth)*, the *Workplace Health and Safety Act 2024*, and the *Privacy Act 1988 (Cth)*, and adheres to the *National Standards for Group Training Organisations* to ensure that access to electronic media is managed in accordance with legal and ethical standards.

PURPOSE

This policy sets out guidelines for acceptable use of Electronic Media Systems and Associated Tools by workers and volunteers of ARU, ensuring compliance with the *Fair Work Act 2009*, *Privacy Act 1988*, and relevant ACNC governance standards

SCOPE

This policy applies to the following, collectively referred to as **'Workers'**:

Employees	Directors	Officers	Contractors (including employees of contractors)	Volunteers
✓	✓	✓	✓	✓

LEGISLATIVE FRAMEWORK

This policy is governed by the following legislation and standards:

- **Fair Work Act 2009 (Cth)** regulates workplace behaviour and acceptable conduct.
- **Privacy Act 1988 (Cth)** outlines obligations for handling personal and sensitive information.
- **Australian Privacy Principles (APPs)** regulate the collection, storage, use and disclosure of personal information.
- **Workplace Surveillance Act 2005 (NSW)** governs computer, camera, and tracking surveillance in the workplace.
- **Work Health and Safety Act 2024 (NSW)** requires ARU to ensure a safe digital working environment.
- **Criminal Code Act 1995 (Cth)** includes offences relating to unauthorised access, modification, or impairment of data and electronic communication.
- **Copyright Act 1968 (Cth)** governs the legal use of digital content.
- **Spam Act 2003 (Cth)** regulates commercial electronic messaging.
- **National Standards for Group Training Organisations (2017)** requires secure information systems and risk controls.
- **Cybersecurity Standards Act 2023 (Cth)** establishes minimum cybersecurity requirements for organisations handling personal or sensitive data.

DEFINITIONS

"**Electronic Media Systems**" includes, but is not limited to:

a) Email
b) Internet
c) Intranet
d) Voicemail
e) Instant messaging and chat facilities, and
f) Online discussion groups

"**Associated Tools**" refers to technology required to access the Electronic Media Systems such as:

a) Phones
b) Computers
c) Tablets

"Monitoring"
Refers to any activity undertaken by ARU to observe, record, review or analyse the use of Electronic Media Systems, including email logs, website activity, keystrokes, files stored, or device activity.

"Surveillance"
Has the meaning set out in the Workplace Surveillance Act 2005 (NSW) and includes computer surveillance, tracking surveillance and camera surveillance undertaken by ARU.

"Personal Use"
Refers to non-work-related use of Electronic Media Systems, limited to infrequent, brief and reasonable activities that do not interfere with work duties or compromise ARU's systems.

"Sensitive Information"
Has the meaning under the Privacy Act 1988 and includes information relating to racial or ethnic origin, religious beliefs, health information, union membership, biometrics and criminal records.

"Cybersecurity"
Refers to the processes, systems, tools and practices used to protect electronic information from unauthorised access, data breaches, malware, loss, or compromise.

POLICY

1. Workers may use Electronic Media Systems and Associated Tools provided by ARU for:
    a) Any work-related purposes.
    b) Limited personal use (for details see *Procedures*, below).
    c) More extended personal use under specific circumstances (for details see *Procedures*, below).
2. Where Workers use Electronic Media Systems and Associated Tools belonging to or paid for by Apprenticeships Are Us Ltd, whether or on off the premises (including when working remotely), properly authorised employees of ARU may access any of those tools or associated data to ensure that the organisation's policies are being adhered to. Such Electronic Media Systems, Associated Tools and data should not be regarded as private in nature.
3. Apprenticeships Are Us Limited may, at its discretion, monitor:
    a) Storage volumes
    b) Internet sites visited

c) Downloaded volumes
d) Suspected malicious viruses
e) [Optional] instant messaging
f) Emails
g) Computer hard drives

ARU may monitor the use of Electronic Media Systems to ensure compliance with this policy. Such monitoring will be conducted in line with the *Privacy Act 1988 (Cth)*, which protects the personal information of employees, and the *Workplace Surveillance Act 2005 (NSW)*, which outlines the conditions under which employee monitoring can be carried out.

MANDATORY WORKPLACE SURVEILLANCE NOTICE

In accordance with the Workplace Surveillance Act 2005 (NSW), ARU hereby notifies all Workers that computer surveillance is in place. This includes monitoring of:

- emails sent and received;
- internet browsing history;
- downloads and uploads;
- files stored on ARU devices;
- device usage, including login times and application activity;
- security alerts, attempted breaches, and flagged content.

Surveillance is ongoing and continuous and applies at all times when ARU Electronic Media Systems or Associated Tools are used, whether onsite, offsite, or during remote work.

This policy must be read in conjunction with:

- ARU Code of Conduct.
- ARU Privacy & Confidentiality Policy.
- ARU Email Retention and Archiving Policy.
- ARU Data Security & Breach Response Procedure.
- ARU Records Management Framework.

COMPANY EQUIPMENT & PROPERTY

All Electronic Media Systems and Associated Tools, such as phones and laptops, supplied by ARU to the Worker, are considered the property of ARU. Workers are responsible for maintaining these tools in good working order, accounting for reasonable wear and tear during their usage.

At the discretion of ARU, Workers may be provided with Associated Tools necessary for the execution of their duties. ARU reserves the right to install programs or software on these tools for purposes of location tracking or monitoring usage. Workers are strictly prohibited from removing such programs or software from the Associated Tools without obtaining prior written approval from ARU.

Furthermore, ARU retains the prerogative to monitor the use of its I.T. equipment at all times, even during remote working arrangements, to ensure compliance with organizational policies and standards.

This policy underscores the ownership of Electronic Media Systems and Associated Tools by ARU and emphasizes the responsibility of Workers to maintain these tools in optimal condition. Additionally, it clarifies the organisation's right to install tracking software for security purposes and its commitment to monitoring I.T. equipment usage to

uphold compliance and safeguard organisational assets. The policy aligns with relevant legislation governing property ownership, data protection, and workplace monitoring practices, ensuring clarity and adherence to legal standards.

All Electronic Media Systems and Associated Tools provided by ARU must be used responsibly. ARU reserves the right to monitor use of its equipment, in compliance with the *Privacy Act 1988*, ensuring that data protection protocols are followed, and all stored information remains secure.

RESPONSIBILITIES

The Managing Director (MD) is responsible for ensuring that all workers understand and adhere to this policy. This includes ensuring compliance with all relevant legislation, including the *Fair Work Act 2009*, *Workplace Health and Safety Act 2024*, and *Privacy Act 1988*.

1. It is the responsibility of the **Managing Director** (MD) to ensure that:
    a) Workers are aware of this policy.
    b) Any breaches of this policy are dealt with appropriately.
2. It is the responsibility of all **Workers** to ensure that their use of Electronic Media Systems and Associated Tools conforms to this policy. Workers are expected to be respectful and professional in all communications using by Apprenticeships Are Us Limited's Electronic Media Systems and Associated Tools.
3. Primary purpose
   Access to Electronic Media Systems and Associated Tools is provided by ARU for the primary purpose of carrying out the tasks and duties associated with a particular role.
4. Limited personal use
   Workers may engage in limited personal use of Electronic Media Systems and associated tools, whether or not they are provided by ARU, in connection with work where it:
    - is infrequent and brief;
    - does not interfere with the duties of the Worker or his/her colleagues;
    - does not interfere with the operation of by ARU;
    - does not compromise the security of ARU or of its systems;
    - does not compromise the reputation or public image of ARU;
    - does not impact on the electronic storage capacity of ARU;
    - does not decrease network performance (e.g., large email attachments can decrease system performance and potentially cause system outages);
    - corresponds to the procedures outlined in the Email Retention and Archiving Policy;
    - conforms to the practices for file management and storage;
    - incurs no additional expense for ARU;
    - violates no laws;
    - does not compromise any of the confidentiality requirements of ARU;
    - does not fall under any of the "unacceptable use" clauses outlined below.

   Examples of what would be considered reasonable personal use are:

    - Conducting a brief online banking transaction or paying a bill.
    - Checking social media during lunchtime.
    - Sending a brief personal email or text or making a brief personal phone call.
5. Permitted extended personal use
   There may be times when Workers need to use the internet or email for extended personal use. An example of this could be when a Workers member needs to use the internet to access a considerable amount of material related to a course they are undertaking. In these situations, it is expected that:

a) The Workers member advises and negotiate this use with their manager beforehand in order to obtain the manager's approval.
b) The time spent on the internet replaces all or part of a Workers member's break/s for that day, or that they adjust their timesheet accordingly for that day.

6. Access to electronic data
   ARU may need to access all Electronic Media Systems and Associated Tools. ARU may authorise particular Workers to inspect any files or messages recorded on its electronic media at any time for any reason. ARU may also recover information that a user has attempted to delete, and Workers should not assume that such data will be treated as confidential.
7. Unacceptable use
   Workers may not use Electronic Media Systems and Associated Tools provided by ARU to:
   - Create or exchange messages that are offensive, harassing, obscene or threatening.
   - Visit websites containing objectionable (including pornographic) or criminal material.
   - Exchange any confidential or sensitive information held by ARU (unless in the authorised course of their duties).
   - Create, store or exchange information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies).
   - Undertake internet-enabled gambling or gaming activities.
   - Conduct a business or side-project.
   - Conduct any illegal activities.
   - Conduct any activities that are not in line with ARU's values.
   - Create or exchange advertisements, solicitations, chain letters or other unsolicited or bulk email.
   - Exchange messages or materials that are discriminatory or violate the Racial Discrimination Act 1975 or Sex Discrimination Act 1984.
   - Engage in any activity that violates the Fair Work Act 2009 or compromises workplace safety under the Work Health and Safety Act 2024.
   - Store or transmit data in breach of the Privacy Act 1988 or Cybersecurity Standards Act 2023.
   - Play games.
8. Security
   Workers must ensure that when not in use, Associated Tools are locked and stored securely. For security reasons, tools should not be left unlocked or unattended in public for any reason. Workers must not leave Associated Tools in a locked vehicle unless ARU has provided prior written approval for this to occur.
9. Security Measures:
   Workers are mandated to adhere to specific security measures concerning the handling and storage of Associated Tools.
   - Locking and Secure Storage: Whenever Associated Tools are not in use; workers are responsible for ensuring these tools are securely locked and stored. This precautionary measure prevents unauthorised access and protects the tools from potential theft or misuse.
   - Avoid Unattended Tools in Public: To maintain security standards, workers should never leave Associated Tools unlocked or unattended in public areas under any circumstances. This practice mitigates the risk of theft or unauthorized use of organizational tools.
   - Vehicle Storage Approval: Workers are prohibited from leaving Associated Tools in a locked vehicle unless explicit prior written approval has been obtained from ARU. This policy ensures that tools are not left vulnerable to theft or misuse in vehicles without organizational authorization.

All workers must comply with ARU's data security protocols, which align with the *Privacy Act 1988* and *Cybersecurity Standards Act 2023*. Any breach of data security, including unauthorized access or loss of data, must be reported immediately. ARU is committed to safeguarding personal and sensitive information and takes breaches of this policy seriously.

CYBERSECURITY OBLIGATIONS

All Workers must adhere to ARU's cybersecurity protocols, including but not limited to:

- using multifactor authentication (MFA) where required
- maintaining strong, unique passwords
- immediately reporting suspected phishing attempts, malware, or unusual activity
- keeping software and security patches updated
- preventing unauthorised access to ARU systems
- complying with the Cybersecurity Standards Act 2023

Workers must not:

- bypass security settings
- install unauthorised software
- connect unapproved personal devices to ARU systems
- disable tracking, antivirus or endpoint protection tools

Failure to comply may result in disciplinary action or legal consequences.

BREACH OF THIS POLICY

Failure to comply with this policy may lead to disciplinary measures, including but not limited to immediate termination of a worker's employment or engagement.

Additionally, disciplinary actions may involve issuing warnings, implementing suspensions, revoking access to the internet, email, and computer usage—either temporarily or permanently—and withdrawing access to the use of Associated Tools.

This policy adheres to relevant workplace legislations and regulations that empower organizations to enforce disciplinary measures in response to breaches of established policies. It aligns with legal frameworks governing workplace conduct, ensuring appropriate consequences for non-compliance and reinforcing the organization's commitment to maintaining standards and adherence to policies.

ACCEPTABLE USE OF ELECTRONIC MEDIA PROCEDURES

RESPONSIBILITIES

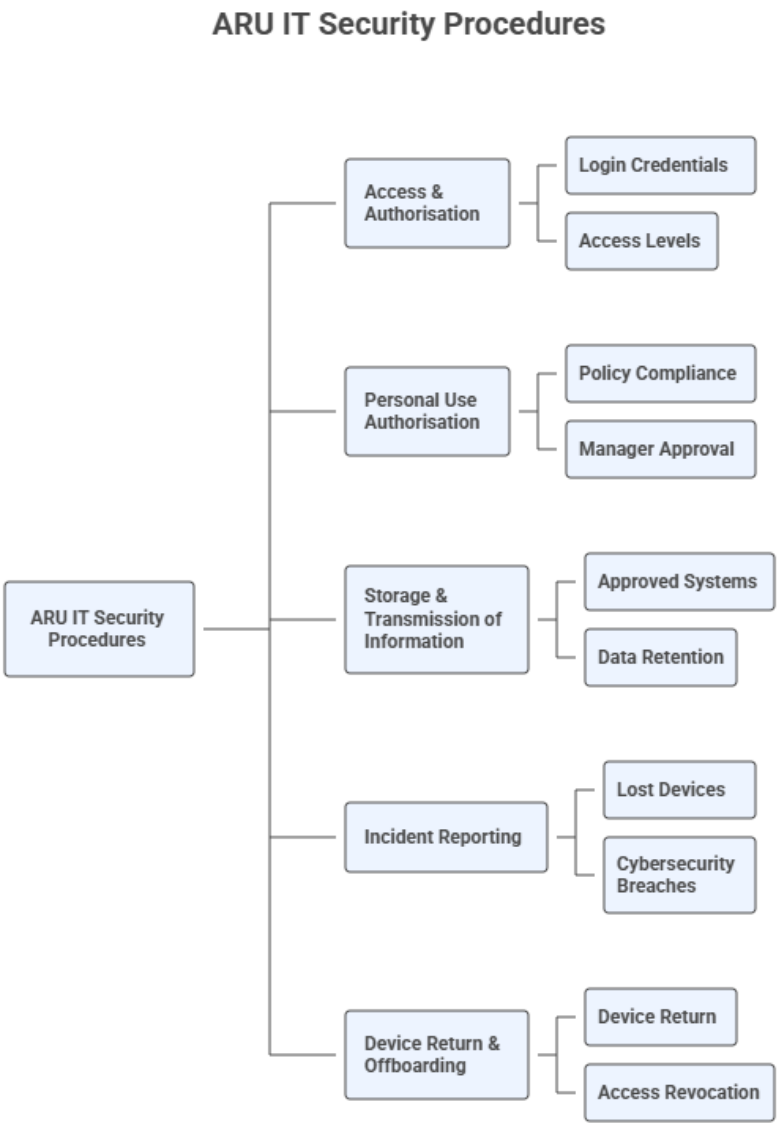
It shall be the responsibility of the MD to implement this policy and to report to the ARU Board annually on its progress.

PROCEDURES

1. All ARU staff shall, wherever feasible, have adequate support and training to provide services and information accessible to all people.
2. ARU will ensure its programs are designed and constructed to provide equal access for all users.
3. ARU, in its role as an employer, will ensure all people have equal access to advertised positions, interviews, equipment, office accommodation, staff training and promotion.
4. ARU shall, wherever feasible, assess proposals for any new (or substantially revised) policies or programs for their direct impact on the lives of people from a range of cultural and linguistic backgrounds prior to any decision to pursue such proposals.
5. Any new (or substantially revised) policies or programs that impact in different ways on the lives of people from different cultural and linguistic backgrounds shall, wherever feasible, be developed by ARU in consultation with people from those backgrounds.
6. ARU shall, wherever feasible, for any new (or substantially revised) policies or program initiatives have a communication strategy developed and sufficiently resourced to inform people from relevant cultural and linguistic backgrounds of these changes.
7. ARU shall provide resources so that publicly available and accessible information on its policies and programs is where necessary communicated appropriately to people from a range of cultural and linguistic backgrounds, and especially to those identified as having a high level of non-compliance.
8. ARU shall institute complaints mechanisms that enable people (regardless of cultural and linguistic backgrounds) to address issues and raise concerns about its performance.
9. ARU shall require that any agents, contractors, or partners of ARU deliver outcomes consistent with this policy, and shall, in bidding for tenders or contracts, budget, where appropriate, for special provision for linguistic and cultural diversity.
10. ARU shall, where necessary and feasible, provide for the special needs of clients from diverse cultural and linguistic backgrounds by providing language assistance through the use of interpreters or facilitators.
11. ARU shall, where necessary and feasible, provide for the special needs of clients in remote areas through developing outreach and community liaison arrangements.
12. ARU shall consider cultural diversity issues in the design and delivery of any training programs it provides.
13. ARU staff shall, where necessary, receive ongoing cultural diversity training so that they develop knowledge and skills to work effectively from a cultural framework.

14. ARU shall, where necessary and feasible, provide information in languages other than English, and through print, electronic media, and disability-appropriate methods of communication.
15. ARU shall, where appropriate, consult with other providers and government agencies to ensure co-ordination of services appropriate to clients' needs.
16. ARU shall promote diversity in the membership of its boards, committees and working groups.
17. ARU shall keep in its client data collection record, where appropriate, such data as birthplace; whether a person's first language spoken was English; Aboriginal or Torres Strait Islander background; Australian South Sea Islander background; date of birth; year of arrival in Australia; birthplace of parents; sex; and religion (the collection of data will not always include all these items, as the relevance of these data items will vary depending on the service delivery context).
18. ARU shall protect the privacy of individual clients when collecting this data. Consideration will be given to:
    - collecting only data essential to the particular service delivery or evaluation purpose;
    - guaranteeing anonymity; and
    - ensuring that all data collection proposals are non-intrusive.

Failure to comply with this policy may result in disciplinary action, including termination of employment or engagement, in accordance with the *Fair Work Act 2009*. Breaches of data protection may also result in legal action under the *Privacy Act 1988* or relevant workplace safety laws.



AUTHORISATION

Michael Wentworth

Managing Director
Apprenticeships Are Us Limited

DOCUMENT CONTROL

Version	Authorised by	Authorisation Date	Sections	Amendment
1.1	M. Wentworth	06/12/2022	All	N/A
1.2	M. Wentworth	28/11/2023	All	Cover page, information update
1.3	M. Wentworth	31/10/2024	All	Information update
1.4	M. Wentworth	25/11/2025	All	Information update