1. Purpose

The purpose of this Policy is to provide a description of how the RTO will respond to a data breach in accordance with the Privacy Act 1988 and Australian Privacy Principles.

2. Policy Statement

Superior Technical College (RTO# 46552 CRICOS # 04444F) (the RTO) is committed to providing quality training and assessment products and services in compliance with the Standards for Registered Training Organisations (RTOs) and all other relevant legislation, including the Privacy Act and Australian Privacy Principles.

It is the RTO's belief that clear roles, responsibilities and procedures will serve as the foundation as a comprehensive privacy program.

This policy outlines:

- the steps that the RTO will take to contain, assess, notify, and review any data breaches that might occur; and
- Notifiable Data Breaches and how the RTO will address them if they occur.

All RTO employees, officers, representatives or advisers ('Employees') are required to understand and act in accordance with this policy.

This policy should be read in conjunction with the Privacy Policy and Records Management Policy and Procedure.

3. Data Breach Definition

A data breach occurs when personal information or intellectual property held by the RTO is subject to unauthorised access, disclosure, modification, or is lost. Data breaches can occur in a number of ways, including but not limited to:

- Unauthorised Third-party security breaches (for example, Hackers)
- Unauthorised access, disclosure or modification by Employees and users
- Data breaches of Third-party services used by the RTO that affect user data
- Specific to the RTO's business, the following have been identified as possible data breach sources:
    - Accidental loss, unauthorised access, or theft of classified material data or equipment on which such the RTO data is stored, such as RTO Laptops and USBs.
    - Unauthorised use, access to, or modification of data on the RTO's SharePoint, Xero, Student Management System, Client Relationship Manager or Learner Management System.

- Accidental disclosure of the RTO user data or intellectual property, such as via email to an incorrect address.
- Unauthorised data collection by third parties posing as the RTO, for example, Phishing Scam
- Failed or successful attempts to gain unauthorised access to the RTO information or information systems
- Unauthorised data collection by third parties through Malware infections on the RTO cloud databases, or hardware equipment.

Clarifying Risk Assessment Criteria for Serious Harm (APP 11.1)

When assessing whether a data breach is likely to result in serious harm, the RTO follows the Office of the Australian Information Commissioner (OAIC) guidelines to evaluate the potential consequences for affected individuals. "Serious harm" extends beyond financial loss and identity theft to include a broad spectrum of risks such as discrimination, psychological distress, reputational damage, workplace disadvantage, and threats to personal safety. For example, if an unauthorised party gains access to sensitive student records, the affected individuals may face employment discrimination if the disclosed information relates to academic performance, disability accommodations, or disciplinary actions. Similarly, if personal contact details such as home addresses or emergency contact information are exposed, this could pose a physical safety risk, particularly in cases of domestic violence or stalking situations.

To determine the likelihood and severity of harm, our RTO conducts a risk assessment considering:

- The nature and sensitivity of the information compromised (e.g., government-issued ID vs. publicly available data).
- The extent of unauthorised access (e.g: a cyberattack exposing thousands of records vs. an accidental disclosure to a trusted third party).
- The potential misuse of the information (e.g: can it be exploited for fraud, social engineering, or discrimination?).
- The affected individual's vulnerability (e.g: minors, international students, or individuals with specific protections such as domestic violence orders).

Where a breach meets the "serious harm" threshold, Superior Technical College will immediately notify the affected individuals and take preventative measures, such as offering identity theft protection services, assisting with legal reporting requirements, and ensuring enhanced security measures are implemented to prevent further risk. This approach ensures compliance with APP 11.1 while protecting students, staff, and stakeholders from undue harm.

4. Retention of Data

The RTO retains data in line with the compliance requirements as outlined in the Records Management Policy and Procedure.

5. Management of Third Party Systems

The RTO recognises that third-party providers, including student management systems, learning platforms, cloud storage services, and external assessment tools, play a critical role in our operations. To maintain compliance with the Privacy Act 1988 (Cth), Australian Privacy Principles (APPs), and relevant state privacy laws, we implement a structured approach to managing third-party compliance. Before engaging a third-party provider, we conduct a privacy and security assessment to ensure that their data protection policies align with our legal obligations. This includes verifying their data storage locations, encryption standards, access controls, and breach response protocols. Additionally, we establish formal agreements (e.g: Service Level Agreements or Data Processing Agreements) that clearly outline their obligations in protecting learner and staff data. We require all third parties to notify us of any data breaches immediately and provide transparency in how personal information is processed. Periodic audits and reviews of third-party providers are conducted to assess ongoing compliance and mitigate potential risks. If a third party fails to meet our security and privacy expectations, we take immediate corrective action, which may include contract termination or transitioning to a more secure provider. This proactive approach ensures that our RTO upholds data security, learner privacy, and regulatory compliance across all external systems and services.

For providers that use aXcelerate, please keep below:

Our primary third party provider is our SMS, aXcelerate is designed with robust security measures to protect user data and ensure system integrity. Key security features include:

- ISO Certifications: aXcelerate is certified under ISO 27001:2022, demonstrating a proactive approach to managing information security risks, and ISO 9001, ensuring continual improvement in quality management processes.
- Data Protection: The platform enforces SSL/TLS protocols for secure communications, encrypts sensitive data at rest, and maintains extensive backup protections with frequent change logs.
- Hosting Environment: Utilising Amazon Web Services (AWS), aXcelerate benefits from on-shore hosting with a 99.9% uptime guarantee, ensuring data is stored securely within Australia.
- Access Controls: The system offers role-based permissions, multi-factor authentication (MFA), and single sign-on (SSO) options to enhance user access security.
- Regular Security Assessments: aXcelerate conducts annual third-party penetration testing and monthly internal vulnerability scans to identify and address potential security issues proactively.

6. What to do if you suspect a data breach has occurred?

All the RTO Employees who are aware of, informed of, or suspect a data breach must inform the RTO's Management and IT team immediately. The IT team must then assess the suspected breach to determine whether or not a breach has in fact occurred. If a data breach has, in fact, occurred, then the IT team will manage the breach according to the steps outlined in the Data Breach Management Plan.

It is important to note that disclosures of data breaches should only come from senior management, if an RTO Employee suspects that a data breach has occurred, this policy does not allow for this information to be shared with other Employees or Clients. This disclosure process must be handled by senior management.

7. Data Breach Response Plan

In accordance with OAIC recommendations, the following steps will be taken in response to a verified Data Breach.

- Contain the breach as soon as possible. Containment is ensuring that the breach itself is stopped. How a breach is stopped would depend on the particular instance but can include:
    - The suspension of compromised accounts;
    - Removal of malware, where identified;
    - Temporary platform downtime if necessary;
    - Recovering any lost data, if possible;
    - Repairing unauthorised modification of data, if possible;
    - Restoring access to the platform when able.
- Assess the risks involved and the repercussions on respective stakeholders. The following may be considered in assessing the stakeholder risks:
    - The type of information involved;
    - Establish the cause and the extent of the breach;
    - Assess the risk of harm to affected persons;
    - Assess the risk of other harms: reputational damage;
    - Notify Management and Affected Individuals and Organisations where appropriate;
    - The CEO is to notify any relevant government entities such as State Training Authorities;
    - Management must be notified of breaches as and when they occur, whether or not the breach is an eligible breach under the Notifiable Data Breach Scheme;
    - the RTO is an APP 11 entity under the Privacy Act 1988 (Cth) and is and must, therefore, comply with its obligations under the Notifiable Data Breach Scheme;
    - Data Breaches that are not eligible under the Notifiable Data Breach Scheme need not be reported and may be addressed internally.
- Prevent future similar breaches through strengthening security infrastructures and/or policies

8. Notifiable Data Breach Scheme

Under the Notifiable Data Breach Scheme, the RTO is obliged to report data breaches that satisfy the following criteria:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the RTO holds (such as USI, IDs, credit card details, and general personal information contained within enrolment forms required by AVETMISS);
- That the unauthorised access to or disclosure of, or loss of personal information is likely to result in serious harm to one or more individuals; and
- the RTO has not been able to prevent the likely risk of serious harm with remedial action.

For further information on how to assess a notifiable data breach, the RTO must refer to the OAIC's APP guidelines.

Where the RTO suspects that an eligible breach has occurred, it must carry out a reasonable and expeditious assessment of the breach: s 26WH(2)(a) of the Privacy Act. Where possible, the assessment must be completed within 30 days of the RTO becoming aware of information that causes it to suspect that an eligible breach has occurred. If the RTO is unable to complete the assessment within 30 days, a written document must be written which addresses:

- how all reasonable steps have been taken to complete the assessment within 30 days;
- the reasons for the delay; and
- that the assessment was reasonable and expeditious.

Where an Eligible Breach has occurred, the RTO must inform affected users AND the Privacy Commissioner. the RTO is allowed to disclose eligible breaches to users in either of the following ways:

- It may notify all the RTO users
- It may notify affected the RTO users
- It may publish a notification on its website

Disclosure of eligible breaches to the Privacy Commissioner may be done by online form.

For more information on disclosing Eligible Breaches under the Notifiable Data Breach Scheme, please refer to the OAIC's webpage on the topic.

9. Disciplinary Consequences

The RTO reserves the right to monitor Employees' use, access and modification of the RTO's data, and initiate an investigation in cases where an employee conducts an action that is in breach of this policy.

All Employees should handle the RTO's data with due diligence in accordance with this policy and any related policies. If an employee's action or omission that is prohibited under this policy causes a disruption of integrity to the data system or leads to a breach defined in the Privacy Act, the employee

may face severe disciplinary action up to and including termination and referral to police or relevant authorities at the discretion of the RTO.

10. Monitoring of Data Security

Note that where an Employee is operating on RTO devices or systems, this information is stored and recorded within the RTOs IT systems and may be recovered or reviewed as required by the RTO. The following are examples of how the company records and keeps information;

- Company emails are recorded and backed up to cloud-based system, the RTO is able to access emails, including deleted emails during and after the Employees period of employment;
- Information about file transfers of documents which are the IP of the RTO are retained and tracked;
- Websites visited on RTO devices are recorded and some sites may be restricted.

11. Legislation

This policy reflects our commitment to the following legislation:

- National Vocational Education and Training Regulator Act 2011 (NVR Act) (Cth)
- The Privacy Act 1988 (Privacy Act) (Cth)
- Cybercrime Act 2001 (Cth)
- Competition and Consumer Act 2010 (Cth)
- Freedom of Information Act 1992 (WA)
- Information Privacy Bill 2007 (WA)
- Privacy and Data Protection Act 2014 (VIC)
- Privacy and Personal Information Protection Act 1998 (NSW)
- Information Privacy Act 2009 (QLD)
- Public Records Act 2002 (QLD)
- Freedom of Information Act 1991 (SA)
- Information Privacy Principles (IPPs) (SA)
- Personal Information Protection Act 2004 (TAS)
- Information Act 2002 (NT)
- Information Privacy Act 2014 (ACT)

12. Monitoring and Improvement

Policy Review

This policy will be reviewed each year and as a standing item, include details of the date it was reviewed and any changes.

- November 2022 - initial creation
- Jan 2025 – Updates against legislation to cover all states; updates to cover determination and monitoring of third party providers; updates as to how aXcelerate/SMS addresses data security; update to consequences for breach of data by staff; updates to clarify criteria for determining serious harm; updates relating to data retention duration.
- November 2025 – Updated roles and responsibilities.

Policy Additions or Amendments

Separate to the mandated annual review, the policy may be varied at any time due to legislative changes or to fall in line with widely accepted best practices in the workplace. In the event of any changes, the policy will be updated, and relevant stakeholders advised.

Shakeel Ahmad, CEO/PEO