EASTCOAST APPRENTICESHIPS

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

Policy: Privacy

Document ID:	Version #:	Release date:	Approval authority:
GEN014 Privacy Policy	1	13/2/2023	CEO
HR-3001	2	17/3/2026	CEO

Table of Contents

1 Introduction and Scope 2
2 Definitions 2
3 Collection and Use of Personal Information 3
4 Sensitive Information 3
5 Financial Information 3
5.1 Purpose of Collecting Financial Information 4
5.2 Storage and Security of Financial Information 4
5.3 Disclosure of Financial Information 4
5.4 Retention, De-identification, and Destruction 5
6 Privacy Protections for Individuals Under 18 5
7 Methods of Collection 6
8 Storage and Data Security 6
9 Data Retention, De-identification and Destruction 6
10 Purpose of Use and Disclosure 7
10.1 Internal Operations: 7
10.2 External Disclosure: 7
11 Overseas Disclosure 7
12 Notifiable Data Breaches 7
12.1 What Constitutes a Breach? 8
12.2 Steps Taken if a Breach Occurs 8
12.3 How Individuals Will Be Notified 8
12.4 Contacts for Urgent Breach Enquiries 8
13 Access, Correction, and Complaints 9
13.1 Access and Correction: 9
13.2 Complaints Handling: 9
14 Policy Governance 9
15 Related Documents 9
16 Document Controls 9
16.1 Document version history 9
16.2 Document review and approval 10
16.3 Key Word indexing 10

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

1 Introduction and Scope

East Coast Apprenticeships (ECA) operates as a Group Training Organisation (GTO) specialising in the employment of apprentices and trainees for placement with Host Employers. As an APP Entity under the *Privacy Act 1988 (Cth)*, we are committed to the transparent and secure management of personal information.

This policy outlines our protocols for collecting, holding, using, disclosing, identifying and destroying personal information—defined as any information or opinion that identifies an individual or makes them reasonably identifiable.

2 Definitions

Personal Information	Information or an opinion relating to an identified person, or someone who can reasonably be identified, regardless of whether the information is accurate or whether it is recorded in any physical or digital form
Sensitive Information	Sensitive information is a specific category of personal information that receives additional protections under the *Privacy Act 1988*. Because improper handling of this type of data can result in discrimination or other significant harm, organisations are generally prohibited from collecting it without your explicit consent. It includes information or opinions about an individual's identity and heritage, beliefs and affiliations, professional memberships, private life, legal history, health information, genetic data, and biometric data
APP Entity (Australian Privacy Principle entity)	An **APP entity** (Australian Privacy Principle entity) is any organisation or agency required to comply with the 13 Australian Privacy Principles under the *Privacy Act 1988*.
Host Employer	A business or organisation that provides an apprentice, trainee, or labour-hire worker with a practical, on-the-job training and work environment
RTO (Registered Training Organisations)	A provider of nationally recognised training and qualifications, registered by the Australian Skills Quality Authority (ASQA) or a state-based regulator
ACAP (Apprentice Connect Australia Provider)	A non-government organisation contracted by the Australian Government to provide free, essential support for the entire lifecycle of an apprenticeship or traineeship
Department of Trade, Employment and Training (DTET)	The state government body responsible for regulating the apprenticeship and traineeship system

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

3 Collection and Use of Personal Information

We collect information strictly necessary to facilitate employment services, vocational training, and corporate operations.

- Stakeholder Groups: Applicants, Program Participants, Apprentices, Trainees, Host Employers, Suppliers, Contractors, and Corporate Staff.
- Data Categories: Names, residential and business addresses, email addresses, telephone numbers, financial/bank details, training progression, and performance information.
- Data Usage: managing employment and payroll, coordinating training and compliance requirements, creating profiles for Host Employers, processing payments and invoices, and monitoring progression against training plans and contracts.

ECA will advise individuals whether requested information is mandatory or optional.

- Mandatory information is required for ECA to carry out core employment, training, payroll, and compliance functions. Without this information, ECA may be unable to:
  - assess suitability for employment or training opportunities
  - establish or maintain an apprenticeship or traineeship
  - process wages, reimbursements, or invoices
  - meet legal and regulatory obligations
- Optional information may enhance the quality of our services or allow us to tailor support. Choosing not to provide optional information will not affect eligibility for employment or training programs.

4 Sensitive Information

Under the *Privacy Act 1988*, "Sensitive Information" includes data regarding racial or ethnic origin, political opinions, religious beliefs, trade union memberships, criminal records, or health information.

ECA will only use sensitive information:

- For the primary purpose for which it was obtained,
- For a secondary purpose directly related to the primary purpose,
- With your explicit consent, or
- Where required or authorised by Australian law.

5 Financial Information

ECA collects certain financial information as part of delivering employment, payroll, and training-related services. Although financial information is not classified as "Sensitive Information" under the Privacy Act 1988, we recognise that many

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

individuals consider this data particularly private and deserving of strong protections. For this reason, ECA treats financial information as a distinct category of personal information and applies enhanced security and retention controls.

5.1 Purpose of Collecting Financial Information

ECA only collects financial information when it is directly required to:

- Process wages, allowances, and reimbursements for apprentices, trainees, and employees
- Make payments to Host Employers, Suppliers, or Contractors
- Comply with taxation, superannuation, and payroll obligations under Australian law
- Meet verification or reporting requirements for Registered Training Organisations (RTOs) or government schemes
- Administer financial transactions associated with training progression or government incentives

We do not use financial information for marketing or unrelated purposes

5.2 Storage and Security of Financial Information

To protect this category of data, ECA applies strict security measures, including:

- Secure digital storage on Australian-based cloud servers with restricted access
- Encryption of financial fields within payroll and finance systems
- Mandatory multi-factor authentication (MFA) for staff accessing payroll or financial records
- Segregation of duties to ensure only authorised finance and payroll personnel can view or modify financial information
- Secure handling of TFNs in accordance with Australian Taxation Office requirements
- Locked storage for any hard-copy financial records

5.3 Disclosure of Financial Information

Financial information is only disclosed:

- To authorised internal staff whose duties require access
- To banks, superannuation funds, or financial institutions strictly for payment processing
- To government agencies (e.g., ATO, DESBT, ASQA) where legally required
- To auditors conducting compliance or financial reviews under confidentiality obligations

We do not disclose financial information to Host Employers, external marketing parties, or unrelated third-party providers.

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

5.4 Retention, De-identification, and Destruction

To maintain compliance with Australian taxation and employment laws:

- Financial records are retained for 5–7 years, depending on statutory requirements
- TFNs and bank details are securely deleted or de-identified when no longer legally required
- Archived records (digital or physical) are securely destroyed through irreversible deletion or certified destruction processes
- De-identified financial data may be retained for internal reporting or statistical purposes where permitted by law

ECA ensures that financial information is never kept longer than necessary and is always treated with heightened care due to its potential risk if misused.

6 Privacy Protections for Individuals Under 18

We employ apprentices and trainees who may be under the age of 18. We are committed to protecting the privacy of young people and ensuring their personal information is handled with appropriate care.

- Capacity to Consent**:** In accordance with Office of the Australian Information Commissioner (OAIC) guidelines, we assess a young person's "capacity to consent" based on their maturity and understanding of how their data will be used.
- Parental/Guardian Consent: While we may presume individuals aged 15 and over have the capacity to consent, we still seek parental or guardian consent before collecting, using, or disclosing personal information.
- Data Handling & Safety: We only collect information from young people that is strictly necessary for their employment, training, or safety (such as contact details, tax file numbers, and emergency contacts). This information is subject to the same high standards of security and limited retention as all other personal data.
- Rights of Parents and Guardians: Where a parent or guardian has provided consent on behalf of a minor, they may also exercise privacy rights on the minor's behalf, including requesting access to or correction of the digital records we hold, until the young person is deemed to have the capacity to manage these rights independently.
- Education and Transparency: We aim to provide privacy notices in plain English that are easy for young workers to understand, ensuring they are empowered to manage their own digital footprint.

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

7 Methods of Collection

ECA collects information through various formal and informal engagement points:

- Digital: Online registrations, email correspondence, and electronic timesheets.
- Verbal: Face-to-face interviews and telephone consultations.
- Physical: Paper-based forms, Host Employer Agreements, and account applications.
- Third Parties: Employment references, resumes, applications through third party platforms including Seek, performance appraisals from Host Employers and academic progress reports from Registered Training Organisations (RTOs).

8 Storage and Data Security

We implement rigorous technical and physical safeguards to protect data from misuse, interference, loss, or unauthorised access:

- Physical Security: Hard-copy records are secured in restricted-access filing cabinets or within a dedicated, locked archive facility with exclusive ECA access.
- Digital Security: Electronic data is hosted on a secure network requiring mandatory password rotations. Sensitive databases require secondary authentication for access.

9 Data Retention, De-identification and Destruction

Physical records are retained for seven years in accordance with the Incorporated Associations Act

We only retain your digital data for as long as it is reasonably necessary for the purposes for which it was collected, or to comply with our legal and regulatory obligations.

- Retention of Digital Data: We maintain digital records of your personal information while you have an active relationship with us, and for a subsequent period required by Australian law (typically between 5 to 7 years for financial, tax, and employment records).
- Sensitive Information: We recognize the heightened risks associated with sensitive information (such as health data or TFNs). Once the specific purpose for which this data was collected has been fulfilled, we will prioritize its secure destruction or de-identification.
- De-identification or Destruction: When your personal or sensitive information is no longer required for a permitted purpose, and we are not legally obligated to retain it, we will take "reasonable steps" to:
    - Destroy the data by irretrievably deleting it from our systems and backups so it can no longer be retrieved.

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

  - De-identify the data by removing or altering identifiers so that the information can no longer be traced back to you. We may keep de-identified data for long-term internal research or statistical purposes where allowed.
- Exceptions: We will not destroy or de-identify your information if we are required by an Australian law or a court/tribunal order to retain it.

10 Purpose of Use and Disclosure

10.1 Internal Operations:

Data is utilised to manage recruitment, monitor on- and off-the-job training, maintain employment records, process financial transactions, and ensure statutory compliance.

10.2 External Disclosure:

- Host Employers: Personal information, including performance and attendance data, is shared with potential and current hosts for placement and workforce management.
- Registered Training Organisations (RTOs): Data is shared to coordinate training plans and monitor educational milestones.
- Apprentice Connect Australia Providers (ACAP) & Government: Information is shared with ACAPs, state training departments (e.g., DESBT), the Australian Skills Quality Authority (ASQA), and relevant funding bodies for compliance, assessment, and auditing.
- Legal Mandates: Information may be disclosed where required or authorised under Australian law.
- Promotional Material: Personal information will only be used for marketing, newsletters, social media, or other promotional content with the individual's prior consent.

11 Overseas Disclosure

ECA does not generally disclose personal information to overseas recipients. While we maintain professional relationships with international organisations, no personal data is transferred outside of Australia without the individual's express written consent. All cloud-hosted data used by ECA is stored on secure, Australian-based servers.

12 Notifiable Data Breaches

We take the security of your digital information seriously. In accordance with the *Privacy Act 1988*, we comply with the Notifiable Data Breaches (NDB) scheme regarding any unauthorised access to your data.

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

12.1 What Constitutes a Breach?

An "Eligible Data Breach" occurs when:

- There is unauthorised access to, unauthorised disclosure of, or loss of personal information held by us.
- This is likely to result in **serious harm** to any of the individuals to whom the information relates.
- We have been unable to prevent the likely risk of serious harm with remedial action.

Serious harm can include identity theft, financial loss, or significant reputational and emotional damage.

12.2 Steps Taken if a Breach Occurs

If we suspect or become aware of a potential data breach, we follow a strict internal response plan:

1. Contain: We take immediate action to contain the breach and limit further access or distribution of data.
2. Assess: We conduct a rapid assessment to determine if the breach is likely to result in serious harm.
3. Remediate: Where possible, we take steps to reduce any potential harm (e.g., remotely wiping a lost device or forcing password resets).
4. Review: Once the incident is resolved, we review our security protocols to prevent a recurrence.

12.3 How Individuals Will Be Notified

If we determine that an Eligible Data Breach has occurred, we will notify you as soon as practicable. Our notification will include:

- A description of the breach.
- The types of information involved.
- Recommended steps you should take in response (e.g., contacting your bank or changing specific passwords).

We will also formally notify the Office of the Australian Information Commissioner (OAIC).

12.4 Contacts for Urgent Breach Enquiries

If you suspect your personal information held by us has been compromised, or if you have received a suspicious communication claiming to be from us, please contact our Risk & Compliance Team immediately:

- Email: admin@ecapprenticeships.com.au
- Phone: 07 3881 3166
- Attention: Risk & Compliance Manager

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

13 Access, Correction, and Complaints

13.1 Access and Correction:

You have the right to request access to the personal information we hold or to request corrections to ensure accuracy. Please direct these requests to the Risk & Compliance Manager at admin@ecapprenticeships.com.au.

13.2 Complaints Handling:

If you believe ECA has breached the Australian Privacy Principles, please submit a written complaint to admin@ecapprenticeships.com.au. Your complaint should include:

1. Your contact details
2. A description of the alleged breach
3. Your requested remedy

ECA will investigate the matter promptly. If you are unsatisfied with our internal resolution, you may escalate the matter to the Office of the Australian Information Commissioner (OAIC).

14 Policy Governance

This policy is reviewed annually to ensure continuous alignment with legislative amendments and evolving industry best practices. It is publicly available on our website. To request a hard copy, please contact the Risk & Compliance team at admin@ecapprenticeships.com.au

15 Related Documents

Doc Type	Document ID	Document title
Policy	HR-5000	Code of Conduct
Policy	RC-2010	Physical & Document Security Policy

16 Document Controls

16.1 Document version history

Version	Release date	Description	Risk-rated review date
1.	13/2/2023	GEN014 Privacy Policy	-
2	17/3/2026	HR-3001 Privacy Policy	17/3/2027

PO Box 5370, Brendale 4500
2 Jockers Street, Strathpine 4500
07 3881 3166

16.2 Document review and approval

Position	Function Owner / author / reviewer / approver
Risk & Compliance Manager	Author
Chief Executive Officer	Approver
Chief Finance Officer	Owner

16.3 Key Word indexing

Keywords:	Privacy; Privacy Act 1988; Personal Information; Sensitive Information; Data Security; Use and Disclosure; Compliance; Access and Complaints