



**PUBLIC**

AVAILABLE ON THE *TURSA* WEBSITE  
OR UPON REQUEST AT A *TURSA* SITE

*Tursa Employment & Training*

**COR003**  
**Privacy Policy**

**5<sup>th</sup> December 2023**

**(Version X)**

WHEN PRINTED THIS DOCUMENT CEASES TO BE CONTROLLED,  
REFER TO *TURSA* WEBSITE OR INTRANET FOR CURRENT VERSION.

## Contents

|  |    |
|--|----|
| Related Documents and References .....   | 3  |
| <b>1.0 PURPOSE</b> .....   | 4  |
| <b>2.0 SCOPE</b> .....   | 4  |
| <b>3.0 Australian Privacy Principles (APPs)</b> .....                                  | 4  |
| <b>4.1 Personal/Sensitive/Protected Information collected by <i>TURSA</i></b> .....    | 4  |
| <b>4.3 Consent to the Collection of Personal/Sensitive/Protected information</b> ..... | 6  |
| <b>4.4 Dealing with Unsolicited Personal/Sensitive/Protected Information</b> .....     | 7  |
| <b>4.5 CCTV Footage and Privacy</b> .....  | 7  |
| <b>4.6 Advice Provided to Individuals</b> .....  | 7  |
| <b>4.7 Use and Disclosure</b> .....  | 7  |
| 4.7.1 Disclosure of Protected Information to Police or other specified agencies.....   | 8  |
| 4.7.1.1 Class PIC .....  | 8  |
| 4.7.1.2 Specific PIC .....   | 9  |
| 4.7.1.3 Subpoenas or Notices to Produce .....  | 9  |
| 4.7.2 Releasing Protected Information to a Third Party (including the police).....     | 9  |
| <b>4.8 Data Quality</b> .....  | 9  |
| <b>4.9 Data Security and Storage</b> .....   | 9  |
| 4.10 Data Availability and Transparency Act 2022 .....                                 | 10 |
| <b>4.11 Use of the Internet</b> .....  | 10 |
| <b>4.12 <i>TURSA</i> website</b> .....   | 11 |
| Passive collection .....   | 11 |
| Active collection .....  | 11 |
| Links to external websites and social networking services .....                        | 11 |
| <b>4.13 Electronic communication</b> .....   | 12 |
| <b>4.14 Digital Platforms</b> .....  | 12 |
| <b>4.15 Access and Correction</b> .....  | 12 |
| <b>4.16 Freedom of Information (FOI) Requests</b> .....                                | 13 |
| <b>4.17 Confirming Identity, Retaining Anonymity and Government Identifiers</b> .....  | 13 |
| <b>5.0 PRIVACY INCIDENTS</b> .....   | 13 |
| <b>5.1 Policy Breach</b> .....   | 13 |
| <b>6.0 PRIVACY COMPLAINTS</b> .....  | 14 |
| <b>7.0 AVAILABILITY of the <i>TURSA</i> PRIVACY POLICY</b> .....                       | 15 |

## Related Documents and References

*Privacy Act 1988 (Privacy Act)*

[Privacy Act 1988 \(Cth\) \(legislation.gov.au\)](https://www.legislation.gov.au/)

*Privacy Amendment (Enhancing Privacy Protection) Act 2012*

<https://www.legislation.gov.au/Details/C2015C00053>

*Australian Privacy Principles 2014 (Privacy Amendment (Enhancing Privacy Protection) Act 2012)*

<https://www.oaic.gov.au/privacy/australian-privacy-principles/>

*Privacy Regulation 2013*

[Privacy Regulation 2013 \(legislation.gov.au\)](https://www.legislation.gov.au/)

*Office of the Australian Information Commissioner*

<https://www.oaic.gov.au/>

*Social Security (Administration) Act 1999*

[Social Security \(Administration\) Act 1999 \(legislation.gov.au\)](https://www.legislation.gov.au/)

[Social Security Act 1991 \(legislation.gov.au\)](https://www.legislation.gov.au/)

[Disability Services Act 1986](https://www.legislation.gov.au/)

NSW Smart and Skilled Contract

Pre-Qualified Supplier Contract – covers both Qld VET Investment Contract and Qld User Choice Contract

Refer to the following documents for the respective Program maintained in the Provider Portal accessed on ECSN secure website:

- o Deeds/Grant Agreement for relevant Privacy, Protected Information and Records Management Instructions (Guideline)
- o Class PIC & Class PIC Instrument of Delegation  
*Social Security (Administration) (Class of Cases) Public Interest Certificate 2022 - Social Security (Administration) Act 1999*, paragraph 208(1)(a), dated 1 July 2022  
<https://ecsnaccess.gov.au/ProviderPortal/Documents/Current/Class-PIC.pdf>  
*Social Security (Administration) (Secretary of the Department of Employment and Workplace Relations) (Disclosure of Information – Class of Cases) Delegation 2022*, dated 1 July 2022, under section 234 of the *Social Security (Administration) Act 1999*  
<https://ecsnaccess.gov.au/ProviderPortal/Documents/Current/Class-PIC-Instrument-of-Delegation>
- o *Social Security (Public Interest Certificate Guidelines) (DSS) Determination 2015*, Disability Employment Services – Class Interest Certificate (No. 2) 2019 (*Disability Services Act 1986 - Section 28(5)(a)*), Social Services (Administration) Act 1999 - Section 208(1)(a) <https://www.legislation.gov.au/Details/F2015L01267>
- o Any other reference material issued under, or in connection with, the respective Deed of Standing Offer/Grant Agreement

## 1.0 PURPOSE

*Tursa Employment & Training* (“*TURSA*”) is committed to protecting the privacy of an individual’s “personal information” and/or “sensitive information”. *TURSA* is bound by the Australian Privacy Principles (*Privacy Amendment (Enhancing Privacy Protection) Act 2012*) that underpin the *Privacy Act 1988*.

This policy sets out the way *TURSA* handles an individual’s personal/sensitive/protected information including the collection, use, disclosure, and storage, as well as the individual’s right to access this information. If *TURSA* changes this Privacy Policy, the document will be updated on the *TURSA* website so as the most current details are available. Accordingly, the *TURSA* website should be referred to for any updates to this Policy.

In relation to any program operated with funding, an individual’s personal information will be treated in accordance with the Queensland [Information Privacy Act 2009 \(Qld\)](#) for funding from the Queensland Government and the [Privacy and Personal Information Protection Act 1998](#) (PPIP Act) for funding from NSW Government and the [Data Provision Requirements 2020](#) as the case may be.

## 2.0 SCOPE

This policy only applies to all *TURSA* staff (including Managers, Board of Directors, and contractors), databases and files and does not cover any State, Territory or Australian Government staff, database, or file. Individuals are advised to contact the relevant government agency for a copy of their privacy policy.

This policy has been developed in accordance with Australian Privacy Principle 1 and operates across all *TURSA*’s contracted employment and training services. It provides understanding of how *TURSA* manages personal and sensitive information, including the access and requested changes, and privacy related complaints under Social Security Law (i.e. the *Social Security Act 1991*, the *Social Security (Administration) Act 1999* and the *Disability Services Act 1986*).

## 3.0 Australian Privacy Principles (APPs)

The APPs, contained in Schedule 1 of the Privacy Act, are principle-based laws that govern the way personal information (including sensitive information) must be handled.

While the APPs are not prescriptive, each APP entity needs to consider how the principles apply to its own situation. This means that *TURSA* must consider its own situation and implement procedures and policies to ensure compliance with the relevant APPs.

For more information on the APPs refer to OAIC’s website [www.oaic.gov.au/privacy/australian-privacy-principles/](http://www.oaic.gov.au/privacy/australian-privacy-principles/)

## 4.0 POLICY

### 4.1 Personal/Sensitive/Protected Information collected by *TURSA*

APP 3 outlines when an APP entity may collect personal information, including sensitive information.

In order to provide employment, training, and assessment services, *TURSA* needs to collect an individual’s personal information (and may include sensitive/protected information) upon registration for a course/qualification, partaking in a project, program, or service to be provided by *TURSA*.

**Personal information** is defined in the Privacy Act as information or an opinion about an identified individual, or an individual who is reasonably identifiable. In order to be personal information, the information or opinion does not need to be true and does not need to be recorded in a material form.

Personal information includes an individual’s name, signature, date of birth, citizenship, address, telephone number, bank account details, employment information, education details and qualifications, and commentary or opinion about an individual. This kind of information may be shared verbally, contained in

physical or digital files or documents, such as résumés or application forms provided by the individual, or in an email or text message, or recorded.

**Sensitive Information** is a subset or type of personal information. It is information or an opinion about an individual's racial or ethnic origin, genetics and biometrics, political opinion or a political association, religious beliefs, memberships of professional or trade associations, sexual preferences or practices, criminal record, and/or medical/health information.

Generally, "sensitive information" has a higher level of privacy protection than "personal information". If *TURSA* assesses any information is sensitive information, an individual's consent will be required for *TURSA* to collect such information.

**Protected information** is defined as "information about a person that was obtained by an officer under the social security law and is held or was held in the records of the relevant government Department/s" – section 23(1) (a) of the Social Security Act 1991 (Cth).

There is no definition of protected information under the *Disability Services Act 1986*, but a person may record or disclose such information in the performance of duties and/or administration of *Disability Services Act 1986* and/or the *Social Security Act 1991*. Such information will generally be both personal and protected information for the purposes of the *Disability Services Act 1983*.

Broadly speaking, this means that personal information about a person who is serviced by *TURSA* is also protected information if the person receives a social security benefit or payment. Such information could include the person's name, date of birth, and contact details.

By having access to this information, *TURSA* and its staff must observe the Social Security Law (i.e. the *Social Security Act 1991*, the *Social Security (Administration) Act 1999* and the *Disability Services Act 1986*) with respect to the collection, use and disclosure of this protected information.

*TURSA* will not collect personal information, including sensitive information, unless this information is reasonably necessary for, or directly related to, the organisation's employment, training and assessment functions and is in line with contractual obligations and legislative requirements.

*TURSA* only collects personal information directly from the individual by fair and lawful means and not in an unreasonably intrusive manner.

The information obtained from Participants may be used to:

- i. assist the individual in securing ongoing employment, work experience and/or education
- ii. identify any potential barriers to employment.

*TURSA* staff are only permitted to tell employers details about a Participant that relate to job opportunities or, with the Participant's permission, their employment with them.

Legislation and government contract conditions require that selected information be reported to government departments and/or agencies. These may include:

- Australian Government departments including the relevant employment services Departments, Services Australia (Centrelink);
- State Governments including NSW Department of Education and QLD's *Department of Education and Department of Employment, Small Business and Training* (DESBT);
- Australian Training Network;
- Australian Vocational Education and Training Management Information Statistical System (AVETMISS); and
- Police and other agencies in circumstances authorised in the Class Public Interest Certificate (PIC) issued by the Secretary of the relevant employment services Departments.

*TURSA* does not disclose personal information to overseas recipients.

## 4.2 Sources of Personal/Sensitive/Protected Information Collected

*TURSA* collects personal information directly from each individual at registration for a course, program, or service, or via an automated system of referral from Australian and State Government information sources, unless any one of the following exceptions applies:

1. the individual consents to the collection of the information from a third party; or
2. *TURSA* is required or authorised by Australian law, or court/tribunal order, to collect the information from the third party; or
3. it is unreasonable or impracticable to collect the personal information directly from the individual.

For example, it may be unreasonable or impracticable to collect personal information directly from an individual where language difficulties prevent the individual from providing their personal information. In these cases, *TURSA* will seek the individual's consent to collect the information through an interpreter or translator. Under APP 10, *TURSA* is required to take reasonable steps to ensure that the collected personal information is accurate, up-to-date, and complete. *TURSA* will take necessary steps to ensure that the interpreter or translator that is used will be providing accurate and complete information from the individual.

*TURSA* will collect this information through completed forms and information provided to us. The enrolment form or program contract completed by the individual contains a disclaimer outlining why the personal information is collected and how it is used. Individuals are required to sign the disclaimer as their agreement to the use of their personal information.

All information collected by *TURSA* is in accordance with the Australian Privacy Principles and will only be disclosed in accordance with these Principles.

Information collected as a result of people browsing *TURSA*'s website is used for monitoring and security purposes only. Cookies may be stored on the website user's computer to assist them to use the website. These are not used for any type of tracking purpose outside of the *TURSA* website.

## 4.3 Consent to the Collection of Personal/Sensitive/Protected information

The primary purpose for the collection of an individual's personal information can be found in the relevant Privacy Notification and Consent Form. *TURSA* may use and disclose an individual's personal information, including sensitive information, for the primary purpose.

During the initial appointment, *TURSA* will seek the individual's express written consent to collect their sensitive information by asking the individual to sign the relevant Privacy Notification and Consent Form, advising the individual that they are not required to give consent for the collection of their sensitive information and can withdraw their consent at any time. Withdrawal will be recorded accordingly, and the Privacy Notification and Consent Form will be kept on file.

While signing the Privacy Notification and Consent Form may indicate express consent at the time of signing, individuals may also provide their express consent to the form verbally or via email if they are unable to sign the form in a Face-to-Face interview.

Where consent is not provided or is withdrawn, *TURSA* cannot collect the individual's sensitive information. If an individual does not consent to the collection of their sensitive information or withdraws their consent to the collection of their sensitive information, the individual will still be required to participate in the relevant program, however, the lack of consent may limit the options and services that a *TURSA* can offer. For example, if a person does not provide consent to the collection of sensitive information about their health status or ethnic origin, they may not be referred to any possible appropriate targeted services.

Where an individual is under 18 years old, *TURSA* will assess if the individual has the capacity to consent on a case-by-case basis. The OAIC advises, as a general rule, that an individual under the age of 18 has the

capacity to consent if they have the maturity to understand what is being proposed. If the individual lacks maturity it may be appropriate for a parent or guardian to consent on their behalf.

#### 4.4 Dealing with Unsolicited Personal/Sensitive/Protected Information

TURSA may receive personal information it did not ask for. APP 4 outlines when TURSA may collect unsolicited personal information. Where TURSA receives unsolicited personal information, we will determine whether it would have been permitted to collect the personal information. If not, TURSA will destroy or de-identify the information unless it is a Commonwealth record under the Archives Act. Most records held by TURSA in performing the Services will be Commonwealth records. TURSA may seek their own independent legal advice prior to destroying unsolicited information.

If TURSA determines that it could have collected the personal information or retains the personal information because it is contained in a Commonwealth record, it will be handled in accordance with the Privacy Act.

#### 4.5 CCTV Footage and Privacy

The personal information which we collect and retain via our CCTV video surveillance will only be used for the purpose of ensuring the safety and security of the building, its contents and its occupants. This is done so in accordance with the Privacy Act (1988), applicable guidelines, relevant State legislation, and organisational policies. For clarity, we will not disclose your personal information, including video footage, to a third party unless you consent, or we are required or authorised by law to do so.

#### 4.6 Advice Provided to Individuals

At the time TURSA collects personal information we will take all reasonable steps to ensure that the individual is made aware of:

1. TURSA's identity and how to contact us
2. The individual's rights with regard to accessing their personal information
3. The purpose for which the personal information was collected
4. To whom we usually disclose an individual's personal information
5. Any law or government contractual obligations that requires us to collect particular personal information
6. The main consequences, if any, for the individual if they do not provide all or part of the information we require and
7. The individual's right of access to the *Cluster, Site or Program Manager* with respect to Customer Complaints - including Privacy matters of concern; an external Customer Complaints hotline, relevant Ombudsman and State/Federal Privacy Commissioners.

#### 4.7 Use and Disclosure

TURSA staff are bound by a policy that all information is used in accordance with the *Commonwealth Privacy Act 1988*, incorporating the *Australian Privacy Principles*. We will endeavour to ensure that the information provided to us remains private and is used only for the agreed purposes (as per completed consent form/s).

TURSA adopts practices to ensure its Personnel are aware of their obligations under the Privacy Act, the applicable Deeds/Grant Agreements/Contracts, and relevant departmental Guidelines. TURSA staff undergo induction that includes privacy training, both TURSA and the relevant Department modules. Staff are also required to complete this applicable privacy training at least once in every subsequent 12 months.

TURSA will not reveal, disclose, sell, distribute, rent, license, share or pass personal information on to a third party, other than those that we have a binding agreement with, ensuring that the third party affords

the personal information similar levels of protection as we do and that allows us to reasonably perform our employment and training and assessment services.

In order to provide an individual with employment, training, and assessment services, we are required to disclose personal information to third parties as outlined in 4.1 of this policy.

Further, *TURSA* may use and disclose personal information to provide employment, training and assessment services specified to the individual at the point of collection or for another purpose if:

- The individual would reasonably expect us to use or disclose it for that purpose
- The use and disclosure is related to the purpose specified to the Individual at the time of collection
- The use and disclosure is specifically authorised by Australian Law or a Court/Tribunal Order
- There is suspected unlawful activity or serious misconduct related to *TURSA*'s activities and functions or
- This is authorised under a Public Interest Certificate (PIC.) See 4.6.1 below.

If an individual is offered paid work and the Employer seeks one or more checks including Police Checks, Working with Children Checks, Working with Vulnerable People Checks, Visa Entitlement Verification Online (VEVO) checks and health/medical checks, the Employer will be directed to source the information directly from the individual.

Where *TURSA* is referring an individual to an activity that requires one or more of these checks, the individual will be referred to the relevant agencies which conduct the checks prior to the placement.

*TURSA* does not use or disclose personal information for the purposes of direct marketing unrelated products or services.

*TURSA* does not send or store any personal information offshore either directly or via Cloud storage.

An individual may be encouraged to provide disability information to prospective employers if relevant to potential employment. *TURSA* staff cannot disclose this information without the individual's consent.

#### **4.7.1 Disclosure of Protected Information to Police or other specified agencies**

Social Security law governs the use and disclosure of protected information for Providers of employment services.

Should a staff member receive a police enquiry for a Participant's information (and the Participant is in receipt of a social security benefit/payment), the information is likely to be considered 'protected' and subject to both privacy law and social security law.

##### **4.7.1.1 Class PIC**

**Certain provisions in social security law enable disclosure of protected information in certain circumstances.**

Section 208 of the Social Security (Administration) Act 1999 makes provision for the Secretary/s of the relevant departments to allow use or disclosure of protected information by issuing a Public Interest Certificate (PIC).

One of the areas where *TURSA* may be authorised to disclose protected information is where the disclosure is authorised by a Public Interest Certificate (PIC). A PIC identifies the information that can be released about a Participant, the purpose for the disclosure and to whom the information can be disclosed. The PIC may also specify who can release the information; and allows the information to be released.

The Class PIC certifies that disclosure is necessary in particular cases, which require the involvement of specific persons (Emergency Services including the Police; emergency call service operators; health service providers; and child protection agencies) and the Participant is unable, refuses, or is likely to refuse to



provide information to those specific persons, for example in the instance of threats or incidents that warrant police attention.

Before disclosing the information, a *TURSA* staff member with the appropriate delegation must consider the facts of the case and determine if the Class PIC applies.

*TURSA* will notify the relevant Department and provide a copy of the request.

#### **4.7.1.2 Specific PIC**

A specific PIC is reserved for situations whereby a Class PIC does not apply and there may be a need to disclose protected information and disclosure is not authorised.

*TURSA* may seek its own legal advice prior to responding to these requests and will contact the relevant employment services Department to obtain a separate specific PIC. This relates to both the *Social Security Administration Act 1999* and the *Disability Services Act 1986*.

#### **4.7.1.3 Subpoenas or Notices to Produce**

Protected information will only be released if requirements regarding protected information under the *Social Security Act* are met. Such requests will be referred to the relevant *Chief Officer* and where required, *TURSA* may seek its own legal advice.

#### **4.7.2 Releasing Protected Information to a Third Party (including the police)**

To meet the Public Interest Certificate (PIC)/Class PIC requirements, only nominated *TURSA* personnel are authorised to disclose personal information about a Participant to the police and must have completed the Department's 'Information Exchange and Privacy' online training.

Release of protected information to a third party outside of certain situations can only occur through a specific Public Interest Certificate (PIC) obtained from the Department.

### **4.8 Data Quality**

*TURSA* will take reasonable steps to ensure that personal information is accurate, complete, up-to-date, relevant, and not misleading.

Individuals are encouraged to help *TURSA* keep their personal information accurate, complete, and up to date by advising their *TURSA* contact, attending one of *TURSA*'s service delivery sites or FREECALL 1800 670 914 to provide any updates to their personal information.

### **4.9 Data Security and Storage**

*TURSA* is committed to protecting the privacy of an individual's personal information. We ensure that all information is stored in accordance with the *Commonwealth Privacy Act 1988* and the *Australian Privacy Principles*.

In accordance with the "digital by default" approach set out in the Australian Government's *Building trust in the public record: managing information and data for government and community policy* (effective 1 January 2021), Providers must, wherever possible and consistent with the Deed/Grant Agreement and other applicable legal requirements, create and manage Records in a digital format.

*TURSA*'s Digital Records are created, stored, and operated in accordance with applicable Deed/Grant Agreement requirements (particularly the requirements in relation to Provider IT Systems and other applicable legislative provisions, including the *Electronic Transactions Act 1999* (Cth)).

We take reasonable steps to protect personal information from misuse, loss, interference and from unauthorised access, modification, or disclosure. We ensure this by having such security measures as:

- Individual password access to systems and databases

- Encrypted electronic databases
- Clear Screen and Clear Desk Policy
- Secured file cabinets

TURSA takes privacy of information very seriously and will at all times take steps to ensure that an individual's information is stored and disposed of securely through the use of and adherence to protected IT systems, filing systems, security procedures, secure offsite storage, and records management policies. Archived personal information is stored in secured premises for time periods as specified by legislation, regulations, or Government contractual obligations. Archived records are in compliance with legislation covering the management of Commonwealth/Deed Records, including the Privacy Act.

TURSA will take reasonable steps to destroy or permanently de-identify personal information if it is no longer required for any purpose and is not required by law to be held for any given period, as per *Archives Act 1983* guidelines.

All TURSA staff are not to remove from, or store outside TURSA's secure network any Participant/Employer/Student personal information using portable storage devices (i.e., USB sticks, portable hard drives), wireless transfers, uploads to personal emails or storage clouds, without express permission from a *Chief Officer*.

#### 4.10 Data Availability and Transparency Act 2022

The *Data Availability and Transparency Act 2022 (Cth)* ('DAT Act') commenced in April 2022. The objectives of the DAT Act are to:

- a) serve the public interest by promoting better availability of public sector data
- b) enable the sharing of public sector data consistently with the *Privacy Act 1988* and use of appropriate security safeguards
- c) enhance integrity and transparency in sharing public sector data
- d) build confidence in the use of public sector data, and
- e) establish institutional arrangements for sharing public sector data.

The DAT Act establishes a data sharing scheme under which Commonwealth bodies are authorised to share their public sector data with accredited users, and accredited users are authorised to collect and use the data, in a controlled way. This can only be used under authorised purposes and the Privacy Act is pivotal to protection of personal information.

TURSA is aware and acknowledges the framework, and does not currently use, store, or share public sector data except for the purposes authorised to deliver employment and training services. Any future participation in the Act by TURSA must be covered pursuant to a formalised data sharing agreement that complies with the Act, with this agreement reviewed and registered in "ICS004 Information Security Register" as maintained by the *Chief Information Security Officer* or delegated IDT staff member.

The *Department of Employment and Workplace Relations* may at any time require TURSA by Notice to provide Public Sector Data to the Department or a third party nominated by the Department for the purposes of sharing that data pursuant to the DAT Act.

'Public Sector Data' is defined in the DAT Act to mean "data lawfully collected, created or held by or on behalf of a Commonwealth body...". Where notified, TURSA will provide the required Public Sector Data within the timeframes and in the manner and form specified by the Department and comply with the relevant data breach provisions of the DAT Act.

#### 4.11 Use of the Internet

TURSA uses a variety of secure technologies to transmit individual personal information from our delivery sites to our head office, and vice versa, and to transmit details to Australian Government registering bodies.

All information transmitted by delivery sites to *TURSA* is encrypted. The security of data transmitted to Australian Government registering bodies is managed by these bodies.

*TURSA* complies with the requirements to protect records containing personal information in accordance with Australian Government security policies, including the Attorney-General's Department's [Protective Security Policy Framework](#) and the Australian Signals Directorate's [Information Security Manual](#). *TURSA* takes all reasonable steps to protect personal information when using the Internet but is aware that no transmission of information by email or via a registering body website can be guaranteed secure.

#### 4.12 *TURSA* website

##### Passive collection

Personal information is collected by a variety of software applications, services and platforms used by your device and by *TURSA* to support the delivery of employment and training services.

This type of information collection is 'passive' as *TURSA* is not collecting this information directly and it does not directly relate to *TURSA*'s provision of services. Your consent for your information to be collected and shared in this way is typically obtained at the time you first use an application or service on your device.

You can opt out of some of these passive data collections, including by:

- disabling / refusing cookies
- disabling JavaScript
- opting out of Google Analytics
- disabling location services on your device.

Additional advice regarding how to protect yourself online can be found at [Stay Secure Online](#).

##### Active collection

Where an individual submits their personal information on the *TURSA* website to provide feedback or via another form, *TURSA* directly collects this information. This information is collected to enable *TURSA* to properly respond and efficiently carry out its functions and deliver services to you.

No attempt is made to identify you through your browsing other than in exceptional circumstances, such as an investigation into the improper use of the website.

| Information may be collected by:  | Type of information:  | Information collected to:   |
|---|---|---|
| Internet browser<br>Cookies<br>Google Analytics<br>Social media platforms | Your browser type<br>Your browser language<br>Your server address<br>Your location (where location services are enabled on your device)<br>Your top-level domain name (e.g. '.com', '.gov', '.au', '.uk')<br>Date and time you accessed a page on our site<br>Pages accessed and documents viewed on our site<br>How our website was accessed (e.g. from a search engine, link, or advertisement) | Measure the effectiveness of our content<br>Better tailor our content to our audience   |
| <i>TURSA</i>  | Name<br>Email address<br>Phone number<br>Education history<br>Employment history  | Deliver services to you<br>Contact you<br>Identify you<br>Subscribe you to a service or update you have requested<br>Evaluate our programs<br>Inform policy development |

##### Links to external websites and social networking services

*TURSA* website includes links to other websites. We are not responsible for the content and privacy practices of other websites. We recommend that you examine each website's privacy policy separately.

We also use social networking services such as Facebook, Google+, LinkedIn and Instagram to engage with the public. When you engage with *TURSA* using these services we may collect your personal information to communicate with you and the public.

The social networking service will also handle your personal information for its own purposes. These services have their own privacy policies. You can access the privacy policies for these services on their websites.

#### **4.13 Electronic communication**

There are inherent risks associated with the transmission of information over the internet, including via email. You should be aware of this when sending personal information to *TURSA* via email or via our website or social media platforms. If this is of concern to you then you may use other methods of communication with us, such as post, or telephone (although these also have risks associated with them).

#### **4.14 Digital Platforms**

*TURSA* uses Swift Digital to manage distribution lists and email subscription services. In order to provide these services, Swift Digital may collect personal information. The personal information collected may include email addresses, and other information to be used for the distribution of email campaigns and other important information.

Swift Digital may also track users' location, device, and operating system, as well as the interaction with the email. The data collected is maintained in compliance with Australia's SPAM Act 2003 and Australia Privacy Provisions.

Swift Digital and its hosted servers are located within Australia. Your personal information collected by Swift Digital will be stored in Australia.

For further information about the type of personal information Swift Digital collects, please refer to [Swift Digital's Privacy Policy](#).

*TURSA* staff may be required to assist Participants by accessing their MyGov account to assist with recording of their Mutual Obligations, job search and other functions under MyGov. In order to do so, staff must obtain appropriate authority from the Participant and/or the relevant Department.

When using digital platforms in a shared space for the purpose of training, participation in activities, job search and recording information to meet Mutual Obligations, *TURSA* will monitor the workstations and remind Participants to log out, collect printouts and be mindful of their private information. Participants are not required to share any personal/sensitive information in a group or a digital environment.

To ensure further privacy, Autofill email function has been removed in *TURSA* Outlook/email systems.

#### **4.15 Access and Correction**

Individuals are provided with the opportunity to access the personal information *TURSA* holds on them and to seek to correct that information if they determine that it is incorrect. *TURSA* will allow any person on whom records are maintained to have access to those records unless Government contractual requirements or legislation (e.g. Freedom of Information Act) requires or authorises the refusal of access.

In some circumstances, such as directions under an Australian law or a court/tribunal order, in cases of serious threat to public or individual health and safety, exceptions to allowing access may be made. These are detailed in the Australian Privacy Principle 12.3.

To obtain access to personal information, the individual is required to make a request at their nearest *TURSA* service delivery site or make a request in writing. Before giving access to information, *TURSA* will

require that the individual provides proof of identification, and this along with details of the request will be recorded on the individual's file.

Correction of personal information/details can be undertaken by the individual contacting their local delivery site or providing details in a written request.

*TURSA* will process requests for access to personal information and requests for correction of personal information and provide a response within 30 days after the request is made.

To request access to CCTV footage the individual is required to make a request at their nearest *TURSA* service delivery site and make a request in writing, which must include their name, contact number and purpose for requesting the CCTV footage. In order to assess the request, *TURSA* will require that the individual provides proof of identification along with details of the request. All supporting documentation for requests/providing CCTV footage to be maintained for audit trail purposes.

#### 4.16 Freedom of Information (FOI) Requests

Under the relevant Deeds/Grant Agreement, *TURSA* is required to assist the relevant Department in processing requests under the FOI Act by providing Records (digital or physical) in their possession that are relevant to a request. An individual seeking to access documents containing their personal information may submit a request for access under either the Privacy Act or the FOI Act. However, where the document being sought does not contain their personal information, access is not available under the Privacy Act as the Privacy Act only applies to personal information.

Requests under the FOI Act will be directed to the relevant Department.

#### 4.17 Confirming Identity, Retaining Anonymity and Government Identifiers

In most instances, it is impractical for *TURSA* to provide a full service to individuals who have not identified themselves or choose to use a pseudonym. It may also be a requirement of law or an Australian Government contract to confirm an individual's identity before providing a full service to them.

*TURSA* is required to use government related identifiers to confirm an individual's identity for the purposes of providing services to the individual and where it is a requirement of a State, Territory or Commonwealth authority. These government identifiers may include state driver's licence, passport, Job Seeker Identification Number, Training Contract Identification Number, Centrelink Client/Student Reference Number, Unique Student Identifier, Tax File Number, Australian Business Number etc.

Where practicable, *TURSA* will not use or disclose an identifier assigned to an individual by a government agency. *TURSA* will not adopt as its own identifier, an identifier that has been assigned by a government agency.

## 5.0 PRIVACY INCIDENTS

In case of privacy breach or a possible privacy breach, *TURSA* is required to:

- **contain** the incident by immediately recovering records or requesting and confirming deletion of electronic information by unintended recipients,
- **investigate** the circumstances, impact, and consequences for Participants,
- **notify** the relevant Department and
- **report** the findings following the investigation to the relevant Department.

### 5.1 Policy Breach

All *TURSA* staff, Managers, Board Directors, and contractors acting on behalf of *TURSA*, must comply with the requirements of this policy.

Any breach of this policy may result in disciplinary action which may include, but is not limited to, issuing a warning, suspension, termination of employment (or, for Persons other than employees, the termination or non-renewal of contractual arrangements).

*TURSA* has developed a *Data Breach Response Plan (DBRP)* based on the OAIC's *Data Breach Preparation and Response - A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*. The purpose of the DBRP is that it outlines the procedures to be followed by *TURSA* staff in the event that *TURSA* experiences a data breach (or suspects that a data breach has occurred) and is essential to facilitate a swift response, ensuring that any legal obligations are met following the data breach. It outlines *TURSA*'s strategy for containing, assessing, and managing a data breach incident from start to finish, setting out clear lines of authority for staff.

The relevant Department has developed the *Breach Management Approach (BMA)*, outlining the principles and approach used by the Department to respond to Breaches and potential Breaches of employment services Deeds or Funding Agreements (as well as any relevant Guidelines) by a Provider, including to determine consistent, appropriate, and proportionate actions required to rectify and remedy a Breach. *TURSA* is to utilise the *Provider Privacy Incident Report* template to notify and report to the Department all cases of unauthorised access to, unauthorised disclosure of or loss of personal information that *TURSA* holds, including that by any of *TURSA*'s personnel.

## 6.0 PRIVACY COMPLAINTS

An individual has the right to report if they believe *TURSA* has not protected their information in line with the Privacy Act 1988 and the Australian Privacy Principles.

The privacy complaint can be made by any of the following:

- visiting the site and speaking to the *Site Manager or Program Manager*
- contacting *TURSA* on FREECALL 1800 670 914
- via the *TURSA* Website [www.tursa.com.au](http://www.tursa.com.au)
- via the Customer Feedback Form (available at the Reception Desk of all *TURSA* servicing sites)
- in writing to:

Customer Feedback  
*TURSA* Management Centre  
PO Box 241  
TWEED HEADS NSW 2485

*TURSA* will respond to any privacy complaints within 30 days and may contact the complainant to:

1. Confirm *TURSA*'s understanding of the conduct complained about or the privacy obligations at issue
2. Advise the investigation process and provide the name, title, and contact details of the staff member handling the complaint
3. Advise how that staff member is independent of the person or persons responsible for the alleged conduct; and
4. Advise when the *TURSA* will contact the complainant again.

After the investigation *TURSA* will respond to the complainant and include an invitation for the complainant to reply and, if appropriate, offer a meeting or discussion.

*TURSA* staff can provide contact details for the Department's external Customer Complaints hotline.

If not satisfied with the response from *TURSA*, individuals may refer to the relevant Ombudsman or the Office of the Australian Information Commissioner, phone 1300 363 992 or on-line to the [Office of Australian Information Commissioner \(OAIC\)](#).

## 7.0 AVAILABILITY of the *TURSA* PRIVACY POLICY

Copies of the *Tursa Employment & Training COR003 Privacy Policy* are available on the organisation's website and hard copies are available on request from service delivery sites.