Australian Government

Privacy Guideline

This Guideline assists Providers who deliver services under any deed that the Department of Education, Skills and Employment (the Department) administers that may refer to this guideline to comply with the Privacy Act 1988 (Privacy Act), including the Australian Privacy Principles (APPs).

The Privacy Act regulates the handling of personal information and sets out principles for the management, collection, use and disclosure of personal information. All APP entities, including the Department, Providers and Host Organisations must comply with the Privacy Act.

This Guideline is not a stand-alone document and does not contain all of Providers' obligations contained in the respective Deed(s). Providers must ensure they comply with:

- the Privacy Act;
- the social security law; and

other legislation or laws relevant to the respective jurisdictions in which they operate, including privacy, work health and safety or anti-discrimination obligations that apply under State or Territory law.

This Guideline is not legal advice and the Commonwealth accepts no liability for any action purportedly taken in reliance upon it. This Guideline does not reduce the obligation of Providers to comply with their relevant legal obligations and, to the extent this Guideline is inconsistent with obligations under the Privacy Act, social security law or any other legislation or laws relevant to the respective jurisdictions in which Providers operate, the Privacy Act, the social security law and the other legislation or laws, respectively, will prevail.

This Guideline must be read in conjunction with the respective Deeds and any relevant Guidelines or reference material issued by the Department under, or in connection with, the respective Deed.

Version: 4.0

Published on: 2 March 2022
Effective from: 7 March 2022

Changes from the previous version (Version 3.1)

Policy changes:

Introduction of requirements related to privacy for Providers, including mandatory annual privacy training requirement for Providers with access to the Department's IT Systems.

Wording changes:

Clarification of information relating to protected information.

Clarification of information relating to collection of information from the Employer Reporting Line.

A full document history and archived guidelines are available on the Provider Portal.

Related documents and references

All Programs

- Complete Privacy Policy
- Records Management Instructions
- Public Interest Certificates – Releasing protected information to a third party (including the police)

Career Transition Assistance

- Guidelines and Supporting Documents

Employability Skills Training

- Guidelines and Supporting Documents

Harvest Trail Services

- Guidelines and Supporting Documents

jobactive

- Guidelines and Supporting Documents

New Enterprises Incentive Scheme (NEIS)

- Guidelines and Supporting Documents

New Employment Services Trial

- Guidelines and Supporting Documents

ParentsNext

- Guidelines and Supporting Documents

Time to Work

- Guidelines and Supporting Documents

Transition to Work

- Guidelines and Supporting Documents

Contents

Definitions

Term	Definition
Administration Act	*Social Security (Administration) Act 1999.*
Archives Act	*Archives Act 1983.*
Agency	Has the same meaning as under the Privacy Act, being any of the following: • a Minister; • a department; • a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being: ▪ an incorporated company, society or association; ▪ an organisation that is registered under the *Fair Work (Registered Organisations) Act 2009* or a branch of such an organisation; ▪ a body established or appointed by the Governor-General, or by a Minister, otherwise than by or under a Commonwealth enactment; ▪ a personal holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a department; ▪ a person holding or performing the duties of an appointment, being an appointment made by the Governor-General, or by a Minister, otherwise than under a Commonwealth enactment; ▪ a federal court; ▪ the Australian Federal Police; ▪ a Norfolk Island agency; ▪ an eligible hearing service provider; or ▪ the service operator under the *Healthcare Identifiers Act 2010.*
APP entity	Has the same meaning as under the Privacy Act, being an agency or organisation.
APPs	The Australian Privacy Principles as set out at Schedule 1 of the Privacy Act.
Consent	Consent may be express consent or implied consent. The four key elements of consent are: • the individual is adequately informed before giving consent; • the individual gives consent voluntarily; • the consent is current and specific, and • the individual has the capacity to understand and communicate their consent. Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.
Data breach	Occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost.

Term	Definition
Deed	Any deed or contract that a Provider delivers employment services under, including the: • jobactive Deed 2015–2022; • Transition to Work Deed 2016–2022; • ParentsNext Deed 2018–2021; • Time to Work Employment Service Deed 2018–2021; • Career Transition Assistance Trial Panel Deed 2018-2022; • Transition Services Panel Deed 2018–2020; and • New Employment Services Trial Deed 2019–2022 In this Guideline all capitalised terms have the same meaning as in the relevant Deed(s).
FOI Act	*Freedom of Information Act 1982*.
Host Organisation	The abbreviation for 'Activity Host Organisation' as defined under the Deeds.
Individual	Has the same meaning as under the Privacy Act, being a natural person.
Lead Provider	A Provider assigned to that role in accordance with the rules set out in the Guidelines.
Loss	Accidental or inadvertent loss of personal information held by an entity, in circumstances where it is likely to result in unauthorised access or disclosure.
Must	Compliance is mandatory.
NDB	Notifiable Data Breach.
OAIC	Office of the Australian Information Commissioner.
Organisation	Has the same meaning as under the Privacy Act, being any of the following: • an individual; • a body corporate; • a partnership; • any other unincorporated association; or • a trust that is not a small business operator, a registered political party, an agency, a State or Territory or a prescribed instrumentality of a State or Territory.
Participant	Has the same meaning as in the relevant Deeds.
PIC	Public Interest Certificate.
Personal Information	Has the same meaning as under the Privacy Act, being information or an opinion about an identified individual, or an individual who is reasonably identifiable: • whether the information or opinion is true or not; and • whether the information or opinion is recorded in a material form or not.
Placements	Referrals to third parties. They include, but are not restricted to: • Paid employment • Work for the Dole Activities • Work Experience (Other) placements • Placements in non-government programs approved for Annual Activity Requirement purposes

Term	Definition
	• Education or training courses • EST Courses • Outbound Visit to an Employer • National Work Experience Placements • Voluntary Work Placements • PaTH Internships • ParentsNext Placements • Transition to Work Placements • Transition Services • Regional Employment Trials Activities • Referrals to non-vocational activities.
Primary purpose	The purpose for which the Provider collects the personal information.
Privacy Act	*Privacy Act 1988* (Cth).
Protected information	Has the same meaning as under the section 23 of the *Social Security Act 1991* (Cth).
Provider/s	An entity contracted to the Commonwealth to provide Services as defined under the Deeds. References to Provider/s will also include references to 'Panel Members' or 'Trial Providers' in certain Deeds.
Secondary purpose	Any purpose that is not the primary purpose.
Sensitive Information	Has the same meaning as under the Privacy Act, being a subset of personal information and is: • information or an opinion about an individual's: ▪ racial or ethnic origin; or ▪ political opinions; or ▪ membership of a political association; or ▪ religious beliefs or affiliations; or ▪ philosophical beliefs; or ▪ membership of a professional or trade association; or ▪ membership of a trade union; or ▪ sexual orientation or practices; or ▪ criminal record; that is also personal information; or • health information about an individual; or • genetic information about an individual that is not otherwise health information; or • biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or • biometric templates.
Serious harm	Serious physical, psychological, emotional, financial, or reputational harm.
Services Australia	The Commonwealth agency of that name at https://www.servicesaustralia.gov.au (formerly the Department of Human Services)
Should	Compliance represents best practice for Providers.
Small business operator	Has the same meaning as under the Privacy Act, being an individual, body corporate, partnership, unincorporated association or trust that: • carries on one or more small business; and

Term	Definition
	• does not carry on a business that is not a small business. A small business operator is not a contracted service provider for a Commonwealth contract (whether or not a party to the contract).
Social Security Act	*Social Security Act 1991* (Cth).
Social security law	The *Social Security Act 1991* (Cth), the *Social Security (Administration) Act 1999* and any other Act that is expressed to form part of social security law.
Unauthorised access	Occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party.
Unauthorised disclosure	Occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the entity.

1. Personal information and sensitive information

'Personal information' is 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.

Common examples of personal information are an individual's name, signature, address, telephone number, date of birth, bank account details, employment details and commentary or opinion about an individual. This kind of information may be contained in paper files or computer systems and in documents provided by the individual, including résumés and application forms.

'Sensitive information' is a subset or type of personal information. Common examples of sensitive information include information about an individual's racial or ethnic origin, information or an opinion about an individual's criminal record and health information about an individual.

Generally speaking, there are additional requirements for collecting, using and disclosing sensitive information. For example, an individual's consent is not required for an APP entity to collect personal information but will be required for an APP entity to collect sensitive information.

2. Australian Privacy Principles

The APPs are principle-based laws that govern the way personal information (including sensitive information) must be handled. The APPs cover:

- the open and transparent management of personal information including having a privacy policy;
- an individual having the option of transacting anonymously or using a pseudonym where practicable;
- the collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection;
- how personal information can be used and disclosed, including overseas;
- maintaining the quality of personal information;
- keeping personal information secure; and

- the right for individuals to access and correct their personal information.

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

For more information on the APPs refer to OAIC's quick reference tool.

3. Collection of personal information and sensitive information

APP 3 outlines when an APP entity may collect personal information, including sensitive information. Generally speaking, it is necessary for Providers to collect personal information in order to deliver the services they are contracted to provide.

The circumstances in which a Provider can collect personal information differ from the circumstances in which a Provider can collect sensitive information, as follows:

- Providers must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the Provider's functions or activities.
- Providers must not collect sensitive information about an individual unless the individual:
  - consents to the collection of the information; and
  - the information is reasonably necessary for, or directly related to, one or more of the Provider's functions or activities.

Consent to the collection of sensitive information

During the initial interview or initial appointment, the Provider must 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. The Provider must advise the individual, during the initial interview or initial appointment, that they are not required to give consent for the collection of their sensitive information and can withdraw their consent at any time.

Where consent is not provided or is withdrawn, the Provider 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 Provider can offer. This must be explained to the individual at the initial interview or appointment. For example, if a person does not provide consent to the collection of sensitive information about their racial or ethnic origin, they may not be referred to any possible appropriate targeted services.

Where an individual withdraws consent to the collection of their sensitive information, the privacy notification and consent form must not be destroyed except in accordance with the Archives Act. The withdrawal of the individual's consent to the collection of their sensitive information must be recorded in the department's IT System.

Information on consent from under 18 year old's can be found at Children and young people — OAIC.

A Provider's activities and functions

A Provider's functions and activities may include but are not necessarily limited to:

- assisting participants to prepare for employment;
- delivering employment services and help to find a job;

- contacting individuals about their participation in the department's programs and, where applicable, their mutual obligation requirements;
- helping to resolve complaints made by individuals or Providers;
- involving individuals in surveys conducted by the department or on behalf of the department; and
- helping to evaluate and monitor the programs and services provided by the department and its contracted Providers.

Manner of collection

Personal information, including sensitive information, must only be collected directly from the individual unless an exception applies. Relevant exceptions which may allow a Provider to collect personal information about an individual from a person other than that individual include where:

- the individual consents to the collection of the information from someone other than the individual; or
- the Provider is required or authorised by Australian law, or court/tribunal order, to collect the information from someone other than the individual; or
- it is unreasonable or impracticable to collect the personal information directly from the individual.

Where a Provider collects information from an individual by use of an interpreter or translator, Providers should seek the individual's consent to the collection of the information from the interpreter or translator, rather than directly from the individual.

The collection of personal information by a Provider must be by lawful and fair means only. A fair means of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive.

Information collected for Employer Reporting Line reports

The Department has a dedicated Employer Reporting Line for employers to report suspected non-compliance by a Participant. In operating the Employer Reporting Line, the Department will collect personal information (and occasionally sensitive information) about Participants, the employer or other individuals. If a report requires action from a Provider, the Department will email an Employer Report Referral (containing personal information) to the Provider.

Providers must follow the instructions contained in the Employer Report Referral, including ensuring that Participants who are the subject of an allegation contained in an Employer Report Referral are notified:

- about the collection of their information by the Department through the Employer Reporting Line,
- that they have a right to respond to the allegation, and
- that no adverse consequences will be imposed until the Department has reviewed the Employer Referral Report (including the Provider's response) and the Participants' response to the allegation.

4. Notifying of the collection of personal information

APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.

APP 5.2 lists a number of matters that must be notified to an individual such as the identity and contact details of the department, the purposes for which the department is collecting the personal information and the main consequences for the individual if all or some of the personal information is not collected by the department.

The purpose of the Privacy Notification and Consent forms attached to this Guideline is to:

- notify individuals of the matters required under APP 5; and
- obtain the individual's consent to the collection of sensitive information as required by APP 3 (see above for further information).

5. Use and Disclosure of personal information

APP 6 provides that if an APP entity holds personal information about an individual that was collected for a particular purpose (primary purpose), the entity must not use or disclose the information for another purpose (secondary purpose) unless an exception applies.

The primary purpose is the purpose for which an APP entity collects personal information. That is, the specific function or activity for which the entity collected the personal information. The primary purpose for the collection of an individual's personal information can be found in the relevant Privacy Notification and Consent Form. A Provider may use and disclose an individual's personal information, including sensitive information, for the primary purpose.

A secondary purpose is any purpose that is not the primary purpose. Providers must not use or disclose personal information, including sensitive information, for a secondary purpose, unless an exception applies.

Relevant exceptions permitting use or disclosure for a secondary purpose include where:

- the individual consents to the use or disclosure*;
- the individual would reasonably expect the use or disclosure, and the secondary purpose is related to the primary purpose or, in the case of sensitive information, directly related to the primary purpose; or
- the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order.

*It should not be assumed that an individual has given consent on the basis alone that they did not object to a proposal to handle personal information in a particular way.

The APP 6 obligations apply to the disclosure of personal information to third parties, that is parties other than the Provider. The Provider may disclose personal information, other than sensitive information, to a related body corporate.

Information for 'checks'

Providers must not disclose personal or sensitive information for the purpose of checks. Examples of 'checks' include: Police Checks, Working with Children Checks, Working with Vulnerable People Checks, Visa entitlement Verification Online (VEVO) checks and health/medical checks.

If an individual is offered paid work and the Employer seeks one or more of these checks, the Employer should source the information directly from the individual.

Where a Provider is referring an individual to an activity that requires one or more of these checks, the Provider must refer the individual to the relevant agencies which conduct the checks prior to the placement.

Location of Services

Services must be delivered at the Provider's premises, another agreed suitable location or as required by the Deed. Services must be held at locations that are accessible, appropriate and safe for Participants, children and Provider staff.

Providers must not conduct Services (including Appointments and other Contacts) at a Participant's home in any circumstance.

A Participant's home address will likely be both personal and protected information, and therefore must only be used by Providers in accordance with this Guideline and with relevant legislation, such as the Privacy Act; the Social Security Act; and the Administration Act.

6. Use and disclosure of protected information

What is protected information?

Protected information is defined in subsection 23(1) of the Social Security Act. Of relevance is paragraph (a) of the definition. It provides that protected information means:

> 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 department or Services Australia.

Therefore, if an individual (who is serviced by an Provider) receives a social security benefit or payment, that individual's information (including their name, date of birth and contact details) will likely be protected information.

Protected information may also be personal information for the purposes of the Privacy Act. For example, the name and contact details of an individual who receives a social security benefit or payment will be both personal and protected information.

Generally speaking, Providers can use and disclose protected information for the purposes of the social security law, such as, for delivering employment services. It is a criminal offence under the Administration Act for a person to intentionally make a record of, disclose to any other person, or otherwise make use of, protected information if the person is not authorised or required under social security law to do so.

Public Interest Certificates

One of the areas where Providers 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, and the purposes for the disclosure and to whom the information can be disclosed. The PIC may also specify who can release the information.

Class PIC

The Department's Secretary has made the *Social Security Administration – Class of Cases – Public Interest Certificate (No. 1) 2020* (the Class PIC).

The Class PIC certifies that disclosure is necessary in particular cases which require the involvement of specific persons (that is, police, ambulance, fire service, and State Emergency Service officers; 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.

The Secretary has delegated the power to disclose information in accordance with the Class PIC to all persons engaged by employment services providers and who have completed the Department's 'Information Exchange and Privacy' online training.

Before disclosing the information, the Provider employee with an appropriate delegation must consider the facts of the case and determine if the Class PIC applies. Employees may consult with their Site Manager (or higher level staff member) to determine if the Class PIC applies, and if so, who may be best placed to disclose the information.

Once the Provider employee has disclosed the information, the employee or the Provider must notify their Account Manager with the Release of Protected Information Notification Form available on the Provider Portal.

For more information on particular cases and the requirements around disclosing protected information under the Class PIC please refer to the Class PIC Factsheet.

Specific PIC

The Secretary and delegates within the Department retain the power to make further PICs to authorise the disclosure of protected information where this is necessary in the public interest (a specific PIC). A specific PIC must be made in accordance with the Minister's guidelines (currently the *Social Security (Administration) (Public Interest Certificate Guidelines) (DEEWR) Determination 2013*).

As a general rule, if satisfied that the Class PIC does not apply, and if there may be a need to disclose protected information and the disclosure is not otherwise authorised such as by the consent of the person, Providers will need to approach the Department through their Account Manager to obtain a specific PIC.

The Provider should seek the specific PIC as soon as possible, outline the reasons why the Provider proposes to disclose the protected information, and why it may not be appropriate to seek the relevant participant's consent to the disclosure.

The Department will not issue a specific PIC in every case and Providers should consult their own legal advisers before responding to the request for protected information.

Subpoenas or notices to produce

If a provider receives a subpoena or a notice to produce from a court which requires disclosure of protected information, the provider must ensure that they comply with all relevant laws, as well as the requirements of the Deed and guidelines, in responding to that subpoena or notice to produce.

In particular, Providers should have regard to section 207 of the Social Security (Administration) Act 1999 in determining whether a Participant's protected information can be disclosed.

Providers should obtain their own legal advice, where relevant.

7. Access to or correction of personal information

Under APP 12, if an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information. APP 12 does not stipulate any formal requirements for making a request, or require that a request to access personal information be made in writing or require an individual to state that it is an APP 12 request. Therefore, a verbal request for personal information may be a valid request under APP 12.

Under APP 13, if an APP entity holds personal information about an individual and the individual requests the entity to correct the information, the entity must take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Generally, Providers must process requests for access to personal information and requests for correction of personal information. If a Provider receives such a request, they must provide a response within 30 days after the request is made.

In accordance with the Deeds, certain requests must be directed to the department for consideration where they encompass records containing information falling within the following categories:

- records also containing information about another person;
- medical/psychiatric records (other than those actually supplied by the individual, or where it is clear that the individual has a copy or has previously sighted a copy of the records);
- psychological records; and
- information provided by other third parties.

If an individual is seeking access to personal information on behalf of another individual, Providers must obtain written authority from the individual whose personal information is being sought before releasing any documents. At a minimum, an authority should state the individual's name, include a description of the documents that they are authorising the release of, who the documents can be released to and bear the individual's signature.

If the Provider is unable to obtain written authority, they should inform the individual that they must wish to make a request under the *Freedom of Information Act 1982* (FOI Act). Requests under the FOI Act should be directed the department's Information Law Team at FOI@dese.gov.au.

Employment Services Assessment (ESAt)

An ESAt is used by DHS to identify if an individual has multiple or complex barriers to employment and may require more intensive support.

The ESAt report may be released to the person that the report is about except where it contains information that may be prejudicial to the health of the individual as identified by the following statement:

This report does contain information, which if released to the client, might be prejudicial to his/her health.

If the individual requests an ESAt report that contains the above statement, the individual should contact the department's Information Law Team at FOI@dese.gov.au to make an FOI request.

8. Privacy breaches

An act or practice of an APP entity that breaches an APP in relation to personal information about an individual is an interference with the privacy of the individual. The Information Commissioner has powers to investigate possible interferences with privacy, either following a complaint by an individual or on the Information Commissioner's own initiative. The Information Commissioner also has a range of enforcement powers and other remedies available.

The Privacy Act requires entities to notify affected individuals and the Information Commissioner about eligible data breaches. An eligible data breach occurs when:

- there is unauthorised access to or disclosure of personal information held by an entity or information is lost in circumstance where unauthorised access or disclosure is likely to occur;
- this is likely to result in serious harm to any of the individuals to whom the information relates; and
- the entity has been unable to prevent the likely risk of serious harm with remedial action.

All potential privacy breaches must be assessed promptly by Providers to determine whether an eligible data breach has occurred and, if required, notification is to be provided to affected individuals and to the OAIC. Providers must take all reasonable steps to ensure that an assessment of a suspected data breach is completed within 30 days of becoming reasonably aware of an eligible data breach.

By responding quickly, a Provider can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.

Under the Deeds, Providers are required to immediately notify the department of any unauthorised access to, or disclosure of, personal information, or a loss of personal information the Provider holds using the Provider Privacy Incident Report at Attachment H (also referenced in the Records Management Instructions). This applies to all breach incidents, whether or not they are an eligible data breach for the purposes of the Notifiable Data Breach (NDB) scheme.

Details about the NDB scheme are available from the OAIC website.

9. Privacy complaints

An individual who considers that their privacy has been interfered with can contact the department and/or OAIC to make a complaint. Generally, complaints under the Privacy Act should be directed to an individual's Provider, where possible.

Providers are required to respond to any privacy complaints within 30 days. Where a Provider receives a privacy complaint, it should:

- Contact the complainant to advise:
    - the Provider's understanding of the conduct complained about;
    - the Provider's understanding of the privacy obligations at issue;
    - that the Provider is conducting an investigation;
    - the name, title and contact details of the Provider staff member handling the complaint;
    - how that staff member is independent of the person or persons responsible for the alleged conduct; and
    - when the Provider will contact the complainant again.
- Conduct an investigation into the issues raised.
- Respond to the complainant and include an invitation for the complainant to reply to the Provider's response and, if appropriate, offer a meeting or discussion.
- Assess any reply or further information from the complainant.
- Consider any systemic issues raised by the complainant and possible responses such as:
    - an apology;
    - privacy training;
    - amendment of policies, forms and/or collection notices;
    - providing additional accessible information;
    - improving security and storage measures; and
    - steps to improve data accuracy.

- Make a record of any changes made and evaluate the changes within 12 months as well as against any future privacy complaints.

10. Referring individuals to the department in relation to privacy matters

An individual can also contact the department to query how their personal information is handled, request access to or correction of their personal information, or make a privacy complaint in relation to the department or a Provider.

Individuals should be provided with the following privacy contact details for the Department, on request:

- By post:

  Privacy Officer
  Information and Corporate Legal Branch
  Location Code C50MA1-LEGAL
  Department of Education, Skill, and Employment
  GPO Box 9880
  Canberra ACT 2601

- By email: Privacy@dese.gov.au
- By telephone: 1300 488 064

For further information refer to the Department of Education, Skills and Employment's Privacy Policy.

11. Privacy Training

Providers must adopt practices to ensure its Personnel are aware of their obligations under the Privacy Act, the Deed and this Guideline. Providers who have access to the Department's IT Systems must ensure that Personnel who handle or will handle personal information in the course of delivering Services under the Deed complete the Department's Information Exchange and Privacy module (Privacy Course), available on the Learning Centre:

- prior to delivering the Services; and
- at least once every 12 months.

Providers should note that the Department's Privacy Course has been developed to cater for the delivery of all employment services. It is not a substitute for any tailored internal privacy training Providers make available to their Personnel. Providers must consider the nature of the employment services they are delivering and Personnel interaction with personal information for those employment services. Where required, Providers must supplement the Department's privacy training with its own training and within the timeframes above.

Information Exchange and Privacy Module

The Privacy Course explains the key concepts under the Privacy Act and the APPs which govern how personal information is collected, used, disclosed, and stored.

The Privacy Course is mandatory and is essential to ensure that Personnel have a comprehensive understanding of this Guideline, the APPs and the social security law, including key processes that help manage potential risks. The completion of mandatory training assists Providers to meet legislative and regulatory requirements, but is not sufficient to meet those requirements.

Privacy resources are also published on the Provider Portal for Personnel to access.

Providers should ensure their internal privacy practices, policies and procedures are proactively reviewed on a bi-annual basis, taking into account compliance with new laws or updated information handling practices, and ensuring that they are responsive to new privacy risks.

Personnel Compliance

Providers must monitor and annually self-audit Personnel completion of privacy training, including the Department's mandatory Privacy Course. The Department may request details of a Provider's self-audit at any time, or may conduct its own audit of a Provider's compliance with the requirements in this Guideline.

Where privacy training is undertaken outside of the Department's Privacy Course on the Learning Centre, the Provider must retain Records of privacy training undertaken by their Personnel and must make this available to the Department on request.

It is also suggested that Providers put in place their own processes to audit the compliance of their Personnel with privacy obligations more generally.

jobactive – PRIVACY NOTIFICATION AND CONSENT FORM

There are two parts to this document:

- **PART A** is to notify you of the collection, use and disclosure of your personal information in accordance with Australian Privacy Principle (APP) 5, and
- **PART B** is to seek your consent to the collection, of your sensitive information in accordance with APP 3.

For information about the Australian Privacy Principles go to the OAIC Australian Privacy Principles webpage.

PART A: NOTIFICATION

PRIVACY STATEMENT

Personal information

Personal information is information about you. Personal information includes a person's name, contact and employment details.

Your personal information is protected by law, including under the *Privacy Act 1988* (Privacy Act).

Collection of your information

Your personal information is, or may have been, collected by your jobactive provider on behalf of the Department of Education, Skills and Employment (the department), other Commonwealth Government agencies (such as Services Australia) and their contracted service providers.

Purpose for collecting your information

Your personal information is collected and used to administer jobactive and provide you with appropriate services and assistance, including:

- contacting you about your participation in jobactive
- delivering jobactive services to you and assistance to help you in your preparation for employment
- evaluating and monitoring the program and services provided to you by the department and your provider
- involving you in surveys conducted by the department or on behalf of the department
- helping to resolve complaints made by you or your provider.

It is important to let your provider know if your circumstances or personal information changes, to ensure you get the right support from your provider.

The department's ability to provide you with appropriate services and assistance may be affected if you do not provide some or all of your personal information.

Disclosure of your information

Your collected personal information may be disclosed to third parties including but not limited to:

- the department's contracted providers
- other Commonwealth Government agencies, and their contracted providers, where those providers are delivering services to you
- other parties who deliver services to you, including Activity Host Organisations
- employers, for example where a provider is arranging a placement for you
- where you agree your personal information can be disclosed to a third party
- where it is otherwise permitted, such as when it is required or authorised by or under an Australian law or a court or tribunal order.

Privacy policy

The department's Privacy Policy can be found on the department's **Privacy page**.

The policy explains how to make a complaint and how to access and correct your personal information**.**

To contact the department about your personal information email **privacy@dese.gov.au.**

PART B: CONSENT TO COLLECT YOUR SENSITIVE INFORMATION

GIVING YOUR CONSENT IS VOLUNTARY

Sensitive information is a subset of 'personal information'. Sensitive information includes, for example, information such as your cultural or linguistic background, religious beliefs, criminal record, health information or membership of professional or trade associations.

The collection of your sensitive information assists providers to tailor services and assistance appropriate to your individual circumstances.
We need your consent to collect your sensitive information. Giving your consent is voluntary.
If you do not give consent, we will not collect your sensitive information. If you do give consent, you can withdraw your consent at any time.
If you do not consent, or if you withdraw your consent, there will be no consequences. You will still need to participate in jobactive but the assistance and services you receive may be limited.

By signing below, I confirm that I have read, understood, and voluntarily agree to the collection of my sensitive information, in accordance with this privacy notification and consent document.

Name: _____

Signature: _____

Date: _____

Declaration by Legal Guardian or Administrator of Participant (where applicable)
I have been appointed the legal guardian or administrator of the Participant and as such, I am authorised to agree to the collection of the Participant's sensitive information in accordance with this document for, and on behalf of, the Participant. **Please tick box: Yes** □

Note: Individuals under the age of 18 are permitted to sign this declaration if they do not have a guardian or administrator appointed. If an individual has an appointed guardian or administrator, the guardian or administrator should sign the declaration.

JOBACTIVE PROVIDER DETAILS

ORGANISATION NAME: _____

PHONE NUMBER OR EMAIL: _____

Transition to Work – PRIVACY NOTIFICATION AND CONSENT FORM

There are two parts to this document:

- **PART A** is to notify you of the collection, use and disclosure of your personal information in accordance with Australian Privacy Principle (APP) 5, and
- **PART B** is to seek your consent to the collection, of your sensitive information in accordance with APP 3.

For information about the Australian Privacy Principles go to the OAIC Australian Privacy Principles webpage.

PART A: NOTIFICATION

PRIVACY STATEMENT

Personal information

Personal information is information about you. Personal information includes a person's name, contact and employment details.

Your personal information is protected by law, including under the *Privacy Act 1988* (Privacy Act).

Collection of your information

Your personal information is, or may have been, collected by your Transition to Work provider on behalf of the Department of Education, Skills and Employment (the department), other Commonwealth Government agencies (such as the Services Australia) and their contracted service providers.

Purpose for collecting your information

Your personal information is collected and used to administer Transition to Work and provide you with appropriate services and assistance, including:

- contacting you about your participation in Transition to Work
- delivering Transition to Work services to you and assistance to help you prepare for employment
- evaluating and monitoring the program and services provided to you by the department and your provider
- involving you in surveys conducted by the department or on behalf of the department
- helping to resolve complaints made by you or your provider.

It is important to let your provider know if your circumstances or personal information changes, to ensure you get the right support from your provider.

The department's ability to provide you with appropriate services and assistance may be affected if you do not provide some or all of your personal information.

Disclosure of your information

Your collected personal information may be collected from and given to third parties including but not limited to:

- the department's contracted providers
- **other Commonwealth Government agencies, and their** contracted providers, where those providers are delivering services to you
- relevant State and Territory Government agencies
- other parties who deliver services to you, which may include Activity Host Organisations, Launch into Work Organisations, employers and education providers, for example where a provider is arranging a placement for you
- where you agree your personal information can be disclosed to a third party
- where it is otherwise permitted, such as when it is required or authorised by or under an Australian law or a court or tribunal order.

Privacy policy

The department's Privacy Policy can be found on the department's **Privacy page**.

The policy explains how to make a complaint and how to access and correct your personal information**.**

To contact the department about your personal information email **privacy@dese.gov.au.**

PART B: CONSENT TO COLLECT YOUR SENSITIVE INFORMATION

GIVING YOUR CONSENT IS VOLUNTARY

Sensitive information is a subset of 'personal information'. Sensitive information includes, for example, information such as your cultural or linguistic background, religious beliefs, criminal record, health information or membership of professional or trade associations.

The collection of your sensitive information assists providers to tailor services and assistance appropriate to your individual circumstances.
We need your consent to collect your sensitive information. Giving your consent is voluntary.
If you do not give consent, we will not collect your sensitive information. If you do give consent, you can withdraw your consent at any time.
If you do not consent, or if you withdraw your consent, the assistance and services you receive may be limited.

By signing below, I confirm that I have read, understood, and voluntarily agree to the collection of my sensitive information, in accordance with this privacy notification and consent document.

Name: _____

Signature: _____

Date: _____

Declaration by Legal Guardian or Administrator of Participant (where applicable)
I have been appointed the legal guardian or administrator of the Participant and as such, I am authorised to agree to the collection of the Participant's sensitive information in accordance with this document for, and on behalf of, the Participant. **Please tick box: Yes** □

Note: Individuals under the age of 18 are permitted to sign this declaration if they do not have a guardian or administrator appointed. If an individual has an appointed guardian or administrator, the guardian or administrator should sign the declaration.

TRANSITION TO WORK PROVIDER DETAILS

ORGANISATION NAME: _____

PHONE NUMBER OR EMAIL: _____

PRIVACY NOTICE AND CONSENT FORM

ParentsNext is an Australian Government program to help you plan your next steps towards study or work. There are two parts to this Privacy Notice and Consent form:

• **PART A** explains how [Provider name] (your provider) and the Department of Education, Skills and Employment (the department), handle your personal information as part of the ParentsNext program.

• **PART B** requests consent for your provider and the department to collect and disclose, where required, your sensitive information. This can be to or from other organisations in order to deliver ParentsNext services.

PART A: PRIVACY NOTICE

Your personal information is protected by law, including under the *Privacy Act 1988* (Privacy Act).

Collection of your information

Your personal information, including your name, contact and employment details, is collected by your ParentsNext provider on behalf of the department, other Commonwealth Government agencies (such as Services Australia) and their contracted service providers. Your personal information may be collected directly from you and/or from third parties (including other organisations and Commonwealth Government agencies).

Purpose for collecting your information

Your personal information is collected and used to administer ParentsNext and provide you with appropriate services and assistance, including:

- contacting you about your participation in ParentsNext
- delivering ParentsNext services to you and assistance to help you prepare for education and employment
- evaluating and monitoring the program and services provided to you by the department and your provider
- involving you in surveys conducted by, or on behalf of, the department about your experience in ParentsNext
- helping to resolve any complaints made by you or your provider.

It is important to let your provider know if your contact details or circumstances change, to ensure you get the right support from your provider.

Your provider's ability to provide you with appropriate services and assistance may be affected if you do not provide some, or all of your personal information.

Disclosure of your information

Your personal information may be disclosed to third parties including but not limited to:

- the department's contracted providers
- other Commonwealth Government agencies, and their contracted providers, where those providers are delivering services to you
- other parties who deliver services to you, including Activity Host Organisations
- employers, for example where a provider is arranging a placement for you
- where you agree your personal information can be disclosed to a third party
- where it is otherwise permitted, such as when it is required or authorised by or under an Australian law or a court or tribunal order.

Privacy policies

Your provider's and the department's privacy policies explain how to access and correct your personal information or make a complaint about how your personal information is used as part of your participation in ParentsNext. Our privacy policies are located at dese.gov.au/privacy and [insert link to provider's privacy web page].

To contact the department about your personal information, email privacy@dese.gov.au.

PART B: CONSENT FORM

As part of your participation in the ParentsNext program, your provider [Provider name] may need to contact other third parties or organisations to help you achieve your education and employment related goals. Other third parties include:

- an interpreter or nominated contact
- community organisations such as family support, or health services
- training and education organisations
- employers or potential employers.

Provider Logo

To tailor services and assistance to your individual circumstances, your provider may need to disclose your personal information to, and collect your personal information from, these organisations.

Any personal information collected by your provider may be accessed by the department to facilitate your participation in the ParentsNext program or assess your provider's performance.

Personal information collected and disclosed may include 'sensitive information', such as your cultural or linguistic background, religious beliefs, criminal record, health information or membership of professional/trade associations.

CONSENT TO COLLECT AND DISCLOSE SENSITIVE INFORMATION

To comply with the Privacy Act, your provider and the department needs your consent to:

- collect your sensitive information
- disclose your sensitive information to third parties, where required.

GIVING YOUR CONSENT IS VOLUNTARY

If you do not give consent, your provider and the department will not collect or disclose your sensitive information unless otherwise permitted under the Privacy Act.

If you do not consent, or if you withdraw your consent, there will be no consequences. While you will still need to participate in ParentsNext, the assistance and services you receive may be limited.

If you do give consent, you can withdraw your consent at any time by contacting your provider.

CONSENT RECORD

By signing below, I agree to:

- my provider and the department collecting and disclosing my sensitive information, including from/to relevant organisations such as community, training and education organisations or employers to receive tailored ParentsNext services and assistance. This authority will remain valid for the duration of your participation in ParentsNext.

☐ Tick the box if you would like to be told the name of the organisation before your sensitive information is collected from, or disclosed to, that organisation.

Name: _____

Signature: _____

Date: _____

Declaration by Legal Guardian or Administrator of Participant (where applicable)

I am the appointed legal guardian or administrator of the Participant and am authorised to agree to provide consent for, and on behalf of, the Participant. **Please tick box: Yes** □

Note: Individuals under the age of 18 can sign this declaration if they do not have a guardian or administrator appointed. If an individual has an appointed guardian or administrator, the guardian or administrator should sign the declaration.

Attachment D – Time to Work Privacy Notification and Consent Forms

Copies of the full range of Time to Work Privacy documents can be found in the Time to Work section of the Provider Portal.

Career Transition Assistance
Privacy Notification and Consent Form

Privacy Statement

Your personal information is protected by law, including the *Privacy Act 1988* (Cth) (Privacy Act). Personal information includes your name, date of birth, contact details, education and employment history and details of your personal circumstances.

Your personal information is collected by your Career Transition Assistance Provider (Provider) on behalf of the Australian Government Department of Education, Skills and Employment(the department) for the purpose of administering Career Transition Assistance (CTA) and provide you with appropriate employment services and support, including:

- delivering CTA services and assistance to you that will help you in your preparation for employment
- evaluating and monitoring the program and services provided to you by the department and its contracted providers
- contacting you about your participation in CTA
- helping to resolve complaints made by you or your Provider
- involving you in surveys conducted by the department or on behalf of the department.

If you do not provide some or all of your personal information, the department may not be able to provide you with suitable employment services and assistance.

Your personal information may be collected from and given to third parties for the purpose of providing you with appropriate services and assistance including:

- the department's contracted providers
- Commonwealth agencies
- relevant State and Territory Government agencies
- contracted providers of other agencies where those providers are delivering services to you
- parties who deliver employment services to you, including Activity Host Organisations and employers.

Your personal information may also be used by the department or given to other third parties where you have agreed, or where it is otherwise permitted, including where it is required or authorised by or under an Australian law, such as social security law, a court or tribunal order, or where a duty of care exists.

Agreement to the collection of sensitive information

In order to provide you with appropriate employment services and support, your Provider may also collect sensitive information, which is a type of personal information. Sensitive information may include details of your cultural or linguistic background, criminal record, membership of a professional or trade association and medical information.

Declaration by Participant:
I agree to the collection of my sensitive information in accordance with this form.

_____ _____
Name Signature

_____
Date

Declaration by Provider:
I declare that I have explained the matters on this form to the Participant, including how their personal and sensitive information will be handled.

_____ _____

Name Signature

_____

Date

More information

The department's Privacy Policy contains more information about how the department will manage your personal information, including information about how you can access your own personal information held by the department and seek correction of such information. The Privacy Policy also contains information on how you can complain about a breach of the Australian Privacy Principles (APP) and how the department will deal with such a complaint. A copy of the department's Privacy Policy can be found on the Privacy page of our website or by requesting a copy from the department via email at privacy@dese.gov.au.

Australian Government

New Employment Services Trial (NEST) – PRIVACY NOTIFICATION AND CONSENT FORM

There are two parts to this document:

- **PART A** is to notify you of the collection, use and disclosure of your personal information in accordance with Australian Privacy Principle (APP) 5, and
- **PART B** is to seek your consent to the collection, of your sensitive information in accordance with APP 3.

For information about the Australian Privacy Principles go to the OAIC Australian Privacy Principles website.

PART A: NOTIFICATION

PRIVACY STATEMENT

Personal information

Personal information is information about you. Personal information includes a person's name, contact and employment details.

Your personal information is protected by law, including under the *Privacy Act 1988* (Privacy Act).

Collection of your information

Your personal information is, may have been, collected by your NEST provider on behalf of the Department of Education, Skills and Employment (the department), other Commonwealth Government agencies (such as Services Australia) and their contracted service providers.

Purpose for collecting your information

Your personal information is collected and used to administer NEST and provide you with appropriate services and assistance, including:

- contacting you about your participation in NEST;
- delivering NEST services to you and assistance to help you in your preparation for employment;
- evaluating and monitoring the program and services provided to you by the department and your Provider;
- involving you in surveys conducted by the department or on behalf of the department; and
- helping to resolve complaints made by you or your provider.

It is important to let your provider know if your circumstances or personal information changes, to ensure you get the right support from your provider.

The department's ability to provide you with appropriate services and assistance may be affected if you do not provide some or all of your personal information

Disclosure of your information

Your collected personal information may be disclosed to third parties including but not limited to:

- the department's contracted Providers;
- other Commonwealth Government agencies, and their contracted providers, where those providers are delivering services to you;
- other parties who deliver services to you, including Activity Host Organisations;
- employers, for example where a provider is arranging a placement for you;
- where you agree your personal information can be disclosed to a third party; or
- where it is otherwise permitted, such as when it is required or authorised by or under an Australian law or a court or tribunal order.

Privacy policy

The department's Privacy Policy can be found on the department's **Privacy page**.

The policy explains how to make a complaint and how to access and correct your personal information**.**

To contact the department about your personal information email **privacy@dese.gov.au.**

PART B: CONSENT TO COLLECT YOUR SENSITIVE INFORMATION

GIVING YOUR CONSENT IS VOLUNTARY

Sensitive information is a subset of 'personal information'. Sensitive information includes, for example, information such as your cultural or linguistic background, religious beliefs, criminal record, health information or membership of professional or trade associations.

The collection of your sensitive information assists providers to tailor services and assistance appropriate to your individual circumstances.
We need your consent to collect your sensitive information. Giving your consent is voluntary.
If you do not give consent, we will not collect your sensitive information. If you do give consent, you can withdraw your consent at any time.
If you do not consent, or if you withdraw your consent, there will be no consequences. You will still need to participate in NEST but the assistance and services you receive may be limited.

By signing below, I confirm that I have read, understood, and voluntarily agree to the collection of my sensitive information, in accordance with this privacy notification and consent document.

Name: _____

Signature: _____

Date: _____

Declaration by Legal Guardian or Administrator of Participant (where applicable)
I have been appointed the legal guardian or administrator of the Participant and as such, I am authorised to agree to the collection of the Participant's sensitive information in accordance with this document for, and on behalf of, the Participant. **Please tick box: Yes** □

Note: Individuals under the age of 18 are permitted to sign this declaration if they do not have a guardian or administrator appointed. If an individual has an appointed guardian or administrator, the guardian or administrator should sign the declaration.

NEST PROVIDER DETAILS

ORGANISATION NAME: _____

PHONE NUMBER OR EMAIL: _____

New Business Assistance with NEIS – PRIVACY NOTIFICATION AND CONSENT FORM

There are two parts to this document:

- **PART A** is to notify you of the collection, use and disclosure of your personal information in accordance with Australian Privacy Principle (APP) 5, and
- **PART B** is to seek your consent to the collection of your sensitive information in accordance with APP 3.

For information about the Australian Privacy Principles go to the OAIC Australian Privacy Principles webpage.

PART A: NOTIFICATION

PRIVACY STATEMENT

Personal information

Personal information is information or an opinion about an individual. Personal information includes an individual's name and contact details.

Personal information is protected by law, including under the *Privacy Act 1988* (Privacy Act).

Collection of your information

Your personal information may be collected by the Department of Education, Skills and Employment ('the department'), your New Business Assistance with NEIS ('NEIS') provider, or by other Commonwealth Government agencies (such as Services Australia) and their contracted service providers.

Purpose for collecting your information

Your personal information is collected and used to administer NEIS services (including Exploring Being My Own Boss Workshops) and provide you with appropriate services and assistance, including:

- determining your eligibility to participate in NEIS
- contacting you about your participation in NEIS
- delivering NEIS services to you
- evaluating and monitoring the program and services provided to you by the department and your provider
- involving you in surveys conducted by the department or on behalf of the department
- helping to resolve complaints made by you or your provider.

It is important to let your provider know if your circumstances or personal information changes, to ensure you get the right support from your provider.

The department's ability to provide you with appropriate services and assistance may be affected if you do not provide some or all of your personal information.

Disclosure of your information

Your collected personal information may be disclosed to third parties including but not limited to:

- the department's contracted providers
- other Commonwealth Government agencies, and their contracted providers, where those providers are delivering services to you
- where you agree your personal information can be disclosed to a third party
- where it is otherwise permitted, such as when it is required or authorised by or under an Australian law or a court or tribunal order.

Personal information you provide about third parties

During your participation in NEIS services you may be asked to provide personal information about other persons, such as the name of business partners that you may have. By providing another person's personal information, you confirm that you have brought this privacy notification to their attention. You can access a copy of this privacy notification on the **department's website**.

Privacy policy

The department's Privacy Policy can be found on the department's **Privacy Page**. The policy explains how to make a complaint and how to access and correct your personal information**.** To contact the department about your personal information email **privacy@dese.gov.au.**

PART B: CONSENT TO COLLECT SENSITIVE INFORMATION

GIVING CONSENT IS VOLUNTARY

Sensitive information is a subset of 'personal information'. Sensitive information includes, for example, information such as your cultural or linguistic background, religious beliefs, criminal record, health information or membership of professional or trade associations.

The collection of your sensitive information assists providers to tailor services and assistance appropriate to your individual circumstances.

We need your consent to collect your sensitive information. Giving your consent is voluntary.
If you do not give consent, we will not collect your sensitive information. You can withdraw your consent at any time. If you do not consent, or if you withdraw your consent you may still participate in NEIS services but the assistance and services you receive may be limited and not tailored to your circumstances.

By signing below, I confirm that I have read, understood, and voluntarily agree to the collection of sensitive information, in accordance with this privacy notification and consent document.

Participant Name: _____

Signature: _____

Date: _____

Declaration by Legal Guardian or Administrator of Participant (where applicable)
I have been appointed the legal guardian or administrator of the Participant and as such, I am authorised to agree to the collection of the Participant's sensitive information in accordance with this document for, and on behalf of, the Participant **Please tick box: Yes** □

Name: _____

Signature: _____

Note: Individuals under the age of 18 are permitted to sign this declaration if they do not have a guardian or administrator appointed. If an individual has an appointed guardian or administrator, the guardian or administrator should sign the declaration.

NEIS PROVIDER DETAILS

ORGANISATION NAME: _____

PHONE NUMBER OR EMAIL: _____

Provider Privacy Incident Report

Use this report to notify the department of unauthorised access to, unauthorised disclosure of or loss of personal information that you hold.

This report is comprised of two parts, an initial report and a detailed report. Part one, the initial report, must be completed and submitted to the department no later than two (2) business days after a privacy incident is identified or brought to your attention. Part two, the detailed report, must be completed and submitted to the department within 30 calendar days after a privacy incident is identified or brought to your attention.

Part one – initial report

Provider details			
Provider name		Provider Org Code	
Details of the person completing the report			
Name		Phone number	
Position		Email address	

Details of the privacy incident	
Describe the privacy incident you are reporting. You should explain who was involved, what happened, why it happened and provide any other information relevant to the context in which it happened.	
Does the privacy incident you are reporting involve the employment services system (ESSWeb)?	Choose an item.
When did the privacy incident occur? You should tell us the time and date, if known.	
When was the privacy incident discovered? You should tell us the time and date, if known.	
How was the privacy incident discovered?	

What kind of personal information was involved in the privacy incident? Select all that apply. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. It does not matter whether the information or opinion is true or not or whether the information or opinion is recorded in a material form or not.					
☐	Names	☐	Opinions, feedback or commentary	☐	Racial or ethnic origin
☐	Signatures	☐	CRNs	☐	Political opinions
☐	Addresses	☐	JSIDs	☐	Membership of a political association
☐	Email addresses	☐	Tax File Numbers	☐	Religious beliefs or affiliations
☐	Dates of birth	☐	Financial information	☐	Philosophical beliefs
☐	Sex or gender	☐	Bank account details	☐	Membership of a trade union or unions
☐	Sexual orientation or practices	☐	Passports	☐	Health information
☐	Criminal record	☐	Drivers' licenses	☐	Genetic or biometric information
If not listed above, specify the other type/s of personal information involved in the privacy incident.					

What was the nature of the privacy incident? Unauthorised access occurs when personal information is accessed by someone who is not permitted to have access. Unauthorised disclosure occurs when personal information is made accessible or visible to others outside of the entity in a way that is not permitted by the *Privacy Act 1988*. Loss occurs when personal information is lost when it is likely to result in unauthorised access or unauthorised disclosure.	Choose an item.
What was the primary cause of the privacy incident? If there are multiple causes of the privacy incident, you should identify only the main cause.	Choose an item.
Was the personal information stored in Australia?	Choose an item.
If 'no', in which country was the personal information stored?	
Was any personal information disclosed or lost overseas?	Choose an item.
At this time, is the privacy incident considered likely to be an eligible data breach under the Notifiable Data Breaches Scheme (NDBS)? An eligible data breach occurs when there is unauthorised access, unauthorised disclosure, or loss of personal information you hold that is likely to result in serious harm to any of the individual to whom the information relates, and you have not been able to prevent the risk of serious harm with remedial action.	Choose an item.
If 'yes', have you discussed your preliminary assessment with your contract manager?	Choose an item.

You should discuss your preliminary assessment with your contract manager before notifying the Office of the Australian Information Commissioner.	
Please provide reasons for your preliminary assessment under the Notifiable Data Breaches Scheme as to why it is or is not an eligible data breach under the NDBS.	

Details of the affected individuals

How many individuals' personal information has been affected by the privacy incident? If the precise number is not known, you should provide an estimate or approximate number.	
Describe the individuals whose personal information has been affected by the privacy incident. For example, employment services participants, employer and/or member of the public.	

Are any of the affected individuals vulnerable? Vulnerable individuals may include children, seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.	Choose an item.
If 'yes', what vulnerabilities have you identified?	
Are any affected individuals in receipt of social security payments and participating in employment services as part of their participation requirements?	Choose an item.
If 'yes, please provide details.	
Did you provide the affected employment services participants, if any, with a copy of relevant privacy notification and consent forms? Please provide a copy of any relevant privacy notification and consent forms.	Choose an item.

Details of initial action

Have any mitigation or rectification actions been taken so far? Mitigation or rectification actions are things that may contain the breach and prevent further harm, such as recalling a misdirected email.	Choose an item.
If 'yes', please describe the mitigation or rectification actions taken to date.	
Will any mitigation or rectification actions be taken in the future?	Choose an item.
If 'yes', please describe the mitigation or rectification actions to be taken in the future, including details of when the actions will be taken.	
Have the affected individuals been notified of this incident? If 'yes', please attach a copy of the relevant notification to this report.	Choose an item.

Has the Office of the Australian Information Commissioner been notified of this incident? If 'yes', please attach a copy of the relevant notification to this report. You should speak to your contract manager before notifying the Office of the Australian Information Commissioner of a privacy incident.	Choose an item.
Has any other entity, such as the police, a security consultant or support team, been notified of this incident?	Choose an item.
If 'yes', please provide details.	

Further information

Is there any further information you wish to provide about this privacy incident?	

Part two – detailed report

Details of investigation

Describe the investigation undertaken. You should explain who was involved in the investigation, what steps were taken, why those steps were taken and any other information relevant to the investigation. You should also provide any supporting evidence or documentation.	

Findings of investigation

Describe the key findings of the investigation.	
What was the nature of the privacy incident? Unauthorised access occurs when personal information is accessed by someone who is not permitted to have access. Unauthorised disclosure occurs when personal information is made accessible or visible to others outside of the entity in a way that is not permitted by the *Privacy Act 1988*. Loss occurs when personal information is lost when it is likely to result in unauthorised access or unauthorised disclosure.	Choose an item.
What was the primary cause of the privacy incident? If there are multiple causes of the privacy incident, you should identify only the main cause.	Choose an item.
Was the personal information stored in Australia?	Choose an item.
If 'no', in which country was the personal information stored?	

Was any personal information disclosed or lost overseas?	Choose an item.
Is the privacy incident considered to be an eligible data breach under the Notifiable Data Breaches Scheme? An eligible data breach occurs when there is unauthorised access, unauthorised disclosure or, loss of personal information you hold that is likely to result in serious harm to any of the individual to whom the information relates, and you have not been able to prevent the risk of serious harm with remedial action.	Choose an item.
If 'yes', have you discussed your assessment with your contract manager? You should discuss your assessment with your contract manager before notifying the Office of the Australian Information Commissioner.	Choose an item.
Please provide reasons for your assessment under the Notifiable Data Breaches Scheme.	
Have the affected individuals been notified of this incident? If 'yes', please attach a copy of the relevant notification and response/s to this report.	Choose an item.
Has the Office of the Australian Information Commissioner (OAIC) been notified of this incident? If 'yes', please attach a copy of the relevant notification to this report. This includes all correspondence until the file is closed with OAIC. You should speak to your contract manager before notifying the Office of the Australian Information Commissioner of a privacy incident.	Choose an item.
Has any other entity, such as the police, a security consultant or support team, been notified of this incident?	Choose an item.
If 'yes', please provide details.	
Details of action taken prior to the incident	
Did you have a Privacy Policy in place? You must have a clearly expressed and up-to-date policy about the management of personal information.	Choose an item.
Did you have policies, practices and/or procedures in place relevant to the incident? You must take such steps as are reasonable in the circumstances to implement practices, procedures and systems that will ensure your compliance with the Australian Privacy Principles.	Choose an item.
If 'yes' please describe the policies, practices and/or procedures in place relevant to the incident?	
Did the relevant staff member/s complete privacy training prior to the incident?	Choose an item.

Staff members who handle personal information are required to complete privacy training on commencement and are recommended to refresh privacy training every 12 months.	
If 'yes' please provide details of all of the privacy training undertaken by the relevant staff members prior to the incident.	

Details of action taken after the incident

Describe the actions taken to contain the incident and prevent harm to the affected individuals.	
Have any further steps been taken to prevent a similar incident occurring in the future?	Choose an item.
If 'yes' please provide details of the steps taken.	
Are any further steps to be taken to prevent a similar incident occurring in the future?	Choose an item.
If 'yes' please detail details of the steps to be taken.	
Have the relevant staff member/s undertaken or retaken the privacy training since the incident occurred? Staff members who handle personal information are required to complete privacy training on commencement and are recommended to refresh privacy training every 12 months or if a privacy incident has occurred.	Choose an item.
If 'yes' please provide details of all of the privacy training undertaken by the relevant staff members since the incident occurred.	

Further information

Is there any further information you wish to provide about this privacy incident?	

Certification

Name of reporting officer	**Signature of reporting officer**	**Date**
Name of CEO	**Signature of CEO**	**Date**