Australian Government

Disability Employment Services

# DES Records Management Instructions and Privacy Guidelines

## V1.0

**Disclaimer**
This document is not a stand-alone document and does not contain the entirety of Disability Employment Services Providers' obligations. It should be read in conjunction with the Disability Employment Services Grant Agreement and any relevant guidelines or reference material issued by the Department of Social Services under or in connection with the Disability Employment Services Grant Agreement.

# Table of Contents

# Records Management Instructions and Privacy Guidelines

### Document Change History

| Version | Effective Date | End Date | Change and Location |
|---|---|---|---|
| 1.0 | 1 January 2023 | | Original version of document. Combined Records Management Instructions and Privacy Guidelines.<br><br>Removal of the Provider Incident Report Form (Refer to Standalone form available on the provider portal).<br><br>Removal of Provider request to return Records Form (Refer to Standalone form available on the provider portal).<br><br>Updated to include the mandatory annual DES privacy training requirements and system block.<br><br>Removal of DES Privacy Notification and Consent Form (Refer to Standalone form available on the provider portal). |

## Records Management Instructions

Overview

The Records Management Instructions (RMI) Guidelines covers Disability Employment Services (DES) Program Providers (hereon referred to as 'Providers') management of identified Agreement Records and includes minimum retention periods under two broad categories:

- Records with retention periods of 6 years ('Priority Records')
- Records with retention periods of 3 years ('General Services Records')

The full description of RMI Records is available at in *Attachment A: Records Retention Periods*.

The RMI provide legally binding instructions for the management, retention and disposal of identified Records created or used by Providers during the delivery of Services under the Disability Employment Services Grant Agreement ('the Agreement') for the Department of Social Services ('the Department'). Providers should read the RMI in conjunction with applicable provisions of the Agreement.

Except as provided for in the next sentence, inactive Records involving Participants under previous contractual arrangements (i.e. prior to the current Agreement) are not included in these RMI and Providers are required to manage these Records in accordance with arrangements in place at that time. The option for Providers to convert paper Records to electronic format as provided at *Section 2: Agreement Records* of these RMI applies to any paper Records created after 1 January 1995, including those created under previous contractual arrangements.

### Disability Employment Services Grant Agreement Clauses:

Section 3D - Records Management
Annexure A - Definitions

## Legislation:

*Archives Act* 1983

## Relevant Agreement Definitions

The Department of Social Services (DSS) administers the DES Program. All references to 'DSS' in the Agreement and any Guidelines, including the definitions extrapolated from the Agreement below, are to be read as references to the 'Department'.

'**Agreement Material**' means all Material:
(a) created for the purpose of performing the Agreement;
(b) incorporated in, supplied or required to be supplied along with the Material referred to in paragraph (a) above; or
(c) copied or derived from Material referred to in paragraphs (a) or (b); and
(d) includes all Agreement Records.

'**Agreement Records**' means all Records:
(a) created for the purpose of performing the Agreement;
(b) incorporated in, supplied or required to be supplied along with the Records referred to in paragraph (a) above; or
(c) copied or derived from Records referred to in paragraphs (a) or (b); and
(d) includes all Reports.

**'Commonwealth Material'** means any Material provided by the Department to the Provider for the purposes of the Agreement and Material that is copied or derived from Material so provided, and includes Commonwealth Records.

**'Commonwealth Records'** means any Records provided by the Department to the Provider for the purposes of the Agreement, and includes Records which are copied or derived from Records so provided.

In addition Commonwealth Records means records generated by the Provider that relate to the funded service (refer to General Records Authority 40 (GRA 40) for further information).

**'Department's IT Systems'** means the IT computer system accessible by a Provider, through which information is exchanged between the Provider, Subcontractors, Services Australia, Services Australia Assessment Services, Ongoing Support Assessors and the Department in relation to the Services.

**'Documentary Evidence'** means those Records of the Provider, as specified in the Agreement including in any Guidelines, which evidence that Services were provided by the Provider for each claim for payment made under the Agreement, or which otherwise support a claim for payment by the Provider.

'**Material**' includes equipment, software (including source code and object code), goods, and Records stored by any means including all copies and extracts of the same.

'**Participant Services Records**' means Agreement Records (including documents associated with the Customer Feedback Register) about a Participant that are directly created for the purposes of providing Services.

'**Provider Records**' means all Records, except Commonwealth Records, in existence prior to the Agreement Commencement Date:
(a) incorporated in;
(b) supplied with, or as part of; or
(c) required to be supplied with, or as part of, the Agreement Records.

'**Records**' means documents, information and data stored by any means and all copies and extracts of the same, and includes Agreement Records, Commonwealth Records and Provider Records.

**Notes:**
It is important to note that the Department owns the Commonwealth Material and Agreement Material but grants the Provider a licence to use, copy and reproduce it for the purposes of the Agreement and in accordance with any conditions or restrictions Notified by the Department to the Provider.

The term 'Commonwealth Records' is used above and throughout this document in a manner that is different to how the term is defined in the *Archives Act 1983*. Under the Archives Act, 'Commonwealth records' are not just those records that are provided by the Commonwealth to the Provider, but rather all records that are the property of the Commonwealth i.e. 'Commonwealth Material' and 'Agreement Material' - (refer to above definition of **''Commonwealth Records'')**. This distinction is relevant to the permission granted by National Archives of Australia for the destruction of Commonwealth records where those records have been converted from hard copy to electronic form (see *Section 2: Agreement Records*).

## Explanatory Notes:

Unless the contrary intention appears, all capitalised terms have the same meaning as in the Agreement. In this document 'must' means that compliance is mandatory; 'should' means that compliance represents best practice.

**These Guidelines should not be read as a stand-alone document. Please refer to the Disability Employment Services Grant Agreement and the National Panel of Assessors Program Grant Agreement.**

## 1. Records Framework

Records can generally be separated into three groups:

- ***Commonwealth Records*** – includes Records provided by the Department to Providers such as the Employment Pathway Plan/Job Plan template or information about a Participant;
- ***Agreement Records*** – includes Records created during the course of providing Services such as Participant Services Records and the Customer Feedback Register; and
- ***Provider Records*** – includes Records in existence prior to the Agreement commencing except for any Commonwealth Records.

The RMI cover only those Records identified in *Attachment A: Records Retention Periods*, wherever they are held in the Provider organisation.

Commonwealth Material (which includes Commonwealth Records) and Agreement Material (which includes Agreement Records) are owned by the Department. Providers have no requirements other than what is specified in the Agreement in relation to Commonwealth Material and Agreement Material.

## 2. Agreement Records

Providers must create accurate Records (including, for example, Participant Services Records) in the course of delivering employment Services. Subject to certain exclusions and conditions, Providers may convert paper Records created on or after 1 January 1995 to electronic form and destroy the originals.

### 2.1 Requirements

Providers may create Records in either paper or electronic form. Arrangements outlined in the RMI cover both forms of a Record. Consistent with the Department's record keeping policy, it is preferred that all Records are created and managed electronically. This is in line with the whole-of-government approach to digital information known as the Building Trust in the Public Record. This policy covers all government information, data and records, as well as systems, services and processes, including those created or delivered by third parties on behalf of Australian Government agencies.

Records that are created electronically should be maintained in digital format. This will ensure that the requirements of the *Electronic Transactions Act 1999* (Cth), and the Agreement are met. Subject to this Section 0, Providers can retain Records in a manner which suits their own business arrangements.

All Commonwealth Material and Agreement Material are 'Commonwealth records' as defined under the *Archives Act 1983* (i.e. records that are the property of the Commonwealth). Subject to certain exclusions and conditions, National Archives provides permission for the destruction of Commonwealth records created on or after 1 January 1995 under General Records Authority 31 (GRA-31) where those records have been converted from hard copy to electronic form. GRA-31 applies to Providers as 'authorised agents' of the Department. Providers must comply with the requirements of GRA-31.

The National Archives may identify a need to suspend the National Archives' records destruction permissions by issuing a records disposal freeze or retention notice. Generally, these state that agencies must not destroy any relevant records. There is currently a disposal freeze on records in relation to violence, abuse, neglect and exploitation of people with a disability.
Further explanation of the relevant exclusions and conditions is provided in the *Guidelines for using General Records Authority 31* issued by the National Archives of Australia. Providers must have regard to these Guidelines in developing any practices and policies for converting paper-based Records into electronic format and, after doing so, in relation to the destruction of the original paper-based Records.

Providers will need to provide access to electronic Records if requested by the Department under the Agreement. For example, Providers must provide direct access to electronic Records in a Provider database or print copies of appropriate screens, if requested by the Department.

Records scanned into an electronic system must also be retained in accordance with the RMI. That is, the scanned information must be retained in accordance with appropriate retention periods.

Information in the Department's IT Systems is an important source of Participant information and will be retained by the Department for the appropriate retention periods.

Refer to *Section 8: Return of Records* for more information on electronic Records.

## 3. Storage of Documentary Evidence in the Department's IT systems

From 1 July 2018 Providers must, at the time a claim for a payment is made, upload to the Department's IT Systems the Documentary Evidence referred to in clause 22.1 of the DES 2018 Grant Agreement as required by any Guidelines, to the Department's satisfaction.

Providers must if requested by the Department, within 10 Business Days of the Department's request, provide to the Department any Documentary Evidence referred to in clause 22.1 that was not uploaded to the Department's IT Systems in accordance with clause 22.2, to the Department's satisfaction.

***THE FOLLOWING INFORMATION APPLIES TO ALL RECORDS THAT ARE NOT REQUIRED TO BE STORED IN THE DEPARTMENT'S IT SYSTEMS, AS PART OF THE REQUIREMENTS OUTLINED AT SECTION 3 ABOVE.***

## 4. Records Storage

Providers must securely store all Records appropriately both on and off-site. All incidents involving inappropriate access, damage, destruction or loss of Records must be reported to the department, to ensure compliance with legislation.

Providers must not transfer Personal Information outside Australia, or allow parties outside Australia to have access to it, without the prior written approval of the Department.

### 4.1 General Storage Requirements

Providers must store Records securely either on their own premises or off-site using a records storage facility in compliance with legislation covering the management of Commonwealth/Agreement Records, for example, the *Privacy Act 1988* outlines arrangements for the management of Personal Information (refer to DES Privacy information below). In addition, Providers are required to store Records in accordance with the department's Security Policies, including *the External Security Policy – For External Service Providers and Users*, available on the IT Security & Access page on the Provider Portal (DES > Key Provider Information> IT Security & Access). Providers must ensure the Department has access to Records if required, either by providing access to a storage facility or by retrieving the Record (including if stored electronically by retrieving the electronic copy and if relevant printing it) and providing it to the Department.

Providers must ensure Records are protected from:

- storage environment damage (e.g. paper Records damp from cement floor)
- unauthorised alteration or removal
- use outside the terms of the Agreement
- breaches of privacy, particularly in relation to Participant Records
- inappropriate 'browsing' of Records by Provider staff or any other person.

Records containing sensitive information as defined in the *Privacy Act 1988*, such as police checks or medical information, must be kept in lockable cabinets or (if electronic) on a secure information system.

Providers may (but are not required to) make paper copies of electronic Records, provided that both paper and electronic Records are stored securely.

## 4.2 Electronic Record Storage Requirements

Providers that choose to store records electronically must ensure that all electronic Record storage systems operate in accordance with the storage and physical access requirements outlined in this RMI and the department's Security Policies.

Where Providers migrate electronic Records to a new storage device or system, or change the file format of an electronic Record, Providers must comply with GRA-31 in destroying the source record (i.e. the original electronic Record). Refer to *Section 2: Agreement Records* for more information on GRA-31.

Providers that choose to outsource the storage of electronic records to a third party should be aware that the requirements outlined in this RMI, the Department's Security Policies, the Agreement or any relevant policy or legislation for the storage of electronic records, applies to third party hosting arrangements. This includes all relevant privacy, security and system requirements.

Providers must not transfer electronic Records to, or store electronic Records with, third party data hosting entities, including cloud storage providers, without the prior written approval of the Department. Where the Department does give such prior written approval, the Provider must comply, and must ensure that the third party data hosting entity complies, with any conditions specified by the Department in providing that approval.

General advice on the management and storage of electronic records and associated metadata is available on the National Archive of Australia website (NAA). The NAA's website provides information on metadata requirements. The metadata should meet the minimum requirements outlined by the NAA. The minimum metadata for records should include an identifier (unique), creator, date created, title, and a protective marking if applicable (such as sensitive or personal privacy).

## 4.3 Reporting Unauthorised Access, Damaged, Destroyed, Lost or Stolen Records

Providers must report all incidents involving unauthorised access, damaged, destroyed, lost or stolen Records to the department as follows:

- notify your Relationship Manager using *Provider Incident Report Form available on the provider portal* no later than the Business Day after the incident.
- report any incidents involving stolen Records to the police immediately.
- make every effort to recover lost or damaged Records (e.g. retrieving or photocopying Records) wherever possible.
  **Note:** damaged Records must not be destroyed without authorisation from the Department.
- if required, arrange and pay for the services of expert contractors (e.g. disaster recovery or professional drying services).
- prepare a detailed report of the incident, including details as appropriate to the incident (e.g. condition of Records – which could include photographs, recovery plans, proposed retrieval action, details of any potential breaches of privacy obligations etc.).
- forward this detailed report to your Relationship Manager as soon as possible and in any case within 15 business days of the incident.
- inform Participants if any Personal Information has been lost or is at risk of being publicly available.
- if necessary, reinterview Participants to recollect information.
- review Record storage standards and access protocols to ensure their adequacy in future. The Department may make recommendations to the Provider to mitigate the risk of re-occurrence of the incident.

## 5. Control of Records

Providers must be able to locate and retrieve Records about a Participant if requested.

Providers must inform their Relationship Manager if they become party to legal action so that arrangements for the appropriate retention of Records can be organised.

### 5.1 Records List

Providers must maintain an up to date list of the Records held by the Provider and make this list available to the Department upon request. This list should contain sufficient information to clearly identify the content and location of a Record in a search process. The list must be created and managed in an electronic format (ideally Microsoft Excel or equivalent or a comma or tab delimited format) that the Department can read.

Providers may wish to identify on the Records list whether Records are:

- Priority – pertaining to current or future legal action (refer below)
- Active – current Participants
- Inactive – former Participants
- Damaged – e.g. paper Record affected by water
- Destroyed – whether authorised or accidental e.g. paper Record burnt
- Transferred – Participant and Record transferred to another Provider
- Returned – Records have been returned to the Department

Examples of Priority Records (also referred to in *Attachment A: Records Retention Periods*) are where the Provider may be aware of the following:

- a complaint
- an injury caused by or to a Participant
- a possible claim for compensation
- current or pending legal action

Refer to *Section 8: Records Retention* for information on the retention of the Records list.

## 6. Transfer of Records

### 6.1 Transfers between Providers

Clause 44.7 of the Agreement provides that, subject to clause 41 [Personal and Protected Information] and clause 62 [Transition Out], Providers must:

(a) not transfer, or be a party to an arrangement for the transfer of custody of the Records to any person, entity or organisation other than to the Department, without the Department's written approval and;

(b) where transferring Records, only transfer the Records in accordance with these Guidelines or as otherwise directed by the Department.

Records must only be transferred between Providers if this is required to continue providing Services to Participants. In such cases, Records must be transferred securely by Providers and as soon as possible and in any case within 28 Business Days of a request to transfer Records. A list of all Records (as per *Section 5.1: Control of Records – Records List*, above) being transferred should be provided to the receiving Provider.

Where the transfer of Records containing Personal Information and Protected Information is permitted under the *Privacy Act 1988* (Cth) and the *Social Security (Administration) Act 1999* respectively, written approval from the Department is not required.

When a Provider is transferring Records off-site to another Provider, for storage, secure destruction or to the Department, it remains the Provider's responsibility to ensure information is secure during the transfer process.

### 6.2 Transfer of Personal Information outside Australia

Providers must not transfer Personal Information outside Australia, or allow parties outside Australia to have access to it, without the prior written approval of the Department.

## 7. Records Retention

Providers must retain Records according to the minimum retention periods outlined in *Attachment A: Records Retention Periods*.

Providers must review Records that have reached the minimum retention period before destroying in accordance with the RMI. If a Record has reached the required minimum retention period but, for example, the Provider has knowledge of legal action or potential legal action, the Record must be re-sentenced[1] (re-appraised) and the Relationship Manager informed.

Retention periods apply to all formats of Records, whether created in paper or electronically or scanned.

**Note:** For purposes of determining the applicable retention period, a scanned version of a paper Record would have the same creation date as the original source document.

Refer to *Section 9: Destruction of Records* for more information on destroying Records.

## 8. Return of Records

Records must be returned to the Department within 28 Business Days if requested by the Department.

Providers must obtain the Department's approval prior to returning any Records to the Department as the return of records will be reviewed on a case-by-case basis as Providers are required to have records management provisions as per the Agreement and as outlined in these Guidelines. Providers may seek permission to return Records to the Department following the Completion Date and should do so by completing *Provider Request to Return Records Form* available on the provider portal and submitting to their Relationship Manager who will verify if records can be returned to the Department. Please note that the request must be accompanied by a list of the Records the Provider is requesting to return.
The following is provided as a guide when returning records to the Department (either requested by the Department or via approval to return):

1. Completion of the *Provider Request to Return Records Form* by the Provider outlining reason for return and particulars of the request;
2. Provider ascertains how many cartons are required to complete the safe retrieval of records;
3. Provider sends the completed *Provider Request to Return Records Form* to their Relationship Manager and include the words "client file returns" and name of provider in the email subject line;
4. Relationship Manager to notify the Department's Information and Records Management Section (IRMS) of the request and forward request details;
5. Approved requests: Collection of records will be coordinated by the IRMS team in conjunction with the Relationship Manager. A detailed procedure will be provided to Providers when needing to return records.
6. Provider to place a supplied 'carton barcode' on the 'short' side of each carton. Papers must be removed from arch files/hard file covers and bundled with file tape/clips instead.

Refer to *Section 5.1: Control of Records – Records List* for information on list requirements.

[1] NAA definition: The process for identifying the disposal class a record belongs to and applying the disposal action specified in the relevant disposal authority. Sentencing is the implementation of decisions made during appraisal.

Providers with a continuing contractual relationship with the Department will be required to manage Records of Participants who have ceased receiving Services in accordance with the previous contractual arrangements in effect at that time. Records of Participants continuing to receive Services are required to be managed in accordance with the Agreement and the RMI.

### 8.1 Electronic Records

Providers creating electronic Records should consider using a format that will allow the Department to read Records if returned to the Department in future. The Department requests that electronic Records be created and managed in Microsoft Office (or the open source equivalent) formats, or in PDF format. The Department will advise Providers if Departmental system requirements change significantly during the Term of the Agreement.

Where electronic participant records are being transferred to the Department, the transfer of these electronic records is done by Kiteworks. Kiteworks is the Department's secure email file transfer system.

Please notify your Relationship Manager via email when your electronic records are ready for transfer. The Relationship Manager will liase with the Department's Records area and further instructions regarding Kiteworks will be provided with a request to the DES provider to upload the relevant files to Kiteworks.

Electronic Records contained in the Department's IT system (the Employment Services System [ESSWeb] do not need to be returned.

### 8.2 Access to Returned Records

Where Records have been returned to the Department and a Provider requires access, the Provider must write to their Relationship Manager with the details and purpose of the request. The Department will consider these requests, but may require Providers to seek access via the freedom of information process as required under the *Freedom of Information Act 1982*.

Where Records have been returned to the Department and a Provider receives an order to produce documents contained in the Records, such as a subpoena, the Provider should seek independent legal advice.

## 9. Destruction of Records

Providers must not destroy or dispose of Records other than in accordance with the RMI or as directed by the Department. When Providers destroy Records, they must use one of the methods outlined below ensuring information is no longer readable and that it cannot be retrieved. Please refer to NAA advice on destruction at the following link.

The destruction of records must comply with the NAA requirements GRA 31.

Records must not be destroyed where Providers are aware of current or potential legal action, even if the minimum retention period is reached. These Records are Priority Records, and must be retained in accordance with requirements set out for Priority Records in *Attachment A: Records Retention Periods*. A Provider must also comply with any direction from the Department not to destroy Records.

Where the relevant records are subject to a disposal freeze (refer to NAA website), providers must mark the relevant records "subject to disposal freeze" to ensure the records are not disposed of, even if the minimum retention period is reached. While the freeze is in place no records relating to the topic or event may be destroyed.

Providers must maintain a list of destroyed Records that must be supplied to the Department upon request. This list must also be retained by the Provider in accordance with the applicable retention period or as directed by the Department.

Refer to *Section 5: Control of Records* for more information on the tracking of Records and *Section 7: Records Retention* for more information on retention periods.

## 9.1 Methods of Destroying Paper-Based Records

Commonwealth policy requires that paper-based Records must only be destroyed using one of the following methods:

- ***Pulping*** – transforming used paper into a moist, slightly cohering mass, from which new paper products will be made;
- ***Burning*** – in accordance with relevant environmental protection restrictions;
- ***Pulverisation*** – using hammermills with rotation steel hammers to pulverise the material;
- ***Disintegration*** – using blades to cut and gradually reduce the waste particle to a given size determined by a removable screen; and
- ***Shredding*** – using crosscut shredders (using either A or B class shredders).

If destruction of paper Records is undertaken at an off-site facility, then a certificate of destruction including details of the Records destroyed and appropriate authorisation, must be obtained and retained by the Provider and a copy provided to the Department's IRMS via the Relationship Manager.

## 9.2 Methods of Destroying Electronic Records

It is a Provider's responsibility to ensure that all electronic Records are identified and removed from systems and destroyed.

Providers, as 'authorised agents' of the Department, must comply with NAA requirements as set out in GRA 31.

Providers need to keep metadata of records to meet the minimum requirements outlined by the NAA.

Electronic Records can only be destroyed using one of the following methods:

- digital file shredding;
- degaussing (i.e. the process of demagnetising magnetic media to erase recorded data); and
- physical destruction of storage media (e.g. pulverisation, incineration or shredding).

Re-formatting may also be used as a method of destroying electronic Records if it can be guaranteed that the process cannot be reversed.

## Attachment A Records Retention Periods

### Records Authority (RA)

The Employment Services Records Authority 2009/00179260 (RA) issued by the National Archives of Australia (NAA), groups together categories of Records with the same minimum retention periods and uses broad terms to assist with the sentencing of Records. The RA gives the legislative framework for the destruction of Records following retention periods as set out in the RMI.

The Records description and examples below help Providers to identify appropriate retention periods based on the type of Record. The numbers included under the 'Entry' heading in each table are the classification numbers from the RA and the term 'last action' is defined as the 'last action taken or the last recorded information' relating to that Record.

The overarching introduction to classifications in the Employment Services RA states:

"The function of implementing labour market programs. Includes managing and coordinating the delivery of employment services and assistance to job seekers; administering the provision of grants and programs to assist targeted groups in the community, such as Indigenous Australians and disadvantaged job seekers; and liaising with local communities."

**Note:** Providers have the discretion to retain Records longer than the minimum periods outlined below, but must not reduce any retention periods. In addition, the Department may direct that some Records be retained for longer periods, for example, in the case of Records required in any legal action.

### RA interpretation

**Priority Records**
Priority Records are specified in Table 1 below. All Priority Records require the utmost attention of Providers to ensure access as required by the Department. In addition to the retention policy below, where there is potential for any legal action, Records must be retained until the matter is resolved.

**Table 1: Priority Records**

| Description of Records | Includes but is not limited to | Disposal action |
|---|---|---|
| Records documenting accidents or incidents to participants engaged in employment services programs, including all relevant records associated with that participant. | ▪ Incident / accident information<br>▪ Potential legal action / fraud Records<br>▪ Customer Feedback Register<br>▪ Risk assessments<br>▪ Other related documentation | Destroy 6 years after last action unless legal action or litigation is underway, in which case the Records must be retained after 6 years until the matter is resolved |
| Register of complaints about pre-employment and employment services, including any and associated documentation. | | |
| Records documenting the services provided to participants engaged in community, voluntary and work experience projects. | | |

**General Services Records**

This category encompasses Records involving the provision of employment Services to Participants. However, if there is any indication that a Record may be required in relation to legal action, the Record must be re-categorised as a Priority Record and managed accordingly.

**Table 2: General Services Records**

| Description of Records | Includes but is not limited to | Disposal action |
|---|---|---|
| Records documenting the processing of project business proposals from participants for assistance under self-employment program schemes, including the assessment of applications, the monitoring and mentoring of participants and records documenting the payment of fees to the providers of these services. | ▪ Employment Pathway Plans<br>▪ Activity agreements<br>▪ Proposed NEIS/Self-Employment Assistance business plans<br>▪ Monitoring / mentoring information<br>▪ Non-work experience placement / service<br>▪ Services and support provided to the Participant<br>▪ Criminal records checks and other background checks<br>▪ Other related documentation | Destroy 3 years after last action |
| Records documenting the successful proposals for all Work Experience activities. Includes receipt, assessment and notification to applicants, project work plans, proposals, outcomes, milestones, performance indicators and successful requests for review of a decision. | | |
| Records documenting the provision of employment services, other than work experience or limited services. | | |

# DES Privacy

## Policy Intent

These Guidelines assist DES Providers with notifying and obtaining consent from DES Participants for collecting, using and disclosing 'personal information', including police, Working with Children and Working with Vulnerable People checks.

All agencies, including the Department of Social Services (Department), Providers, and Host Organisations have obligations under the *Privacy Act 1988* (Cth) (Privacy Act) to ensure that 'personal information' (including sensitive information) is collected, held, used and disclosed in accordance with that Act.

Information that a Provider holds about a Participant will be 'personal information', even if it is only a limited amount of information. The information or opinion does not have to be true and does not have to be recorded in material form. This includes information contained in paper files or computer systems and in documents provided by the Participant, including résumés and application forms. A Provider will also hold other 'personal information' about employers or persons associated with a Host Organisation.

Providers may handle 'sensitive information' including:

- information about a Participant's racial or ethnic origin, such as whether they identify as being Aboriginal or Torres Strait islander
- information about a Participant's criminal convictions such as information on any time served in prison or
- health information about Participants such as information about medical issues.

With limited exceptions under the Privacy Act, a Participant's consent is required for the collection and subsequent use and disclosure of 'sensitive information'**.**

**Disability Employment Services Grant Agreement Clauses:**

Clause 16 - Criminal Records Checks and other measures
Clause 41 - Personal and Protected Information
Clause 44 - Records the Provider must keep
Clause 45 - Access by Participants and Employers to Records held by the Provider
Clause 75.1(a) – Compliance with laws and government policies.
Clause 80.1 – Provision of Program Services

## Legislation:

*Privacy Act 1988* (Privacy Act)
*Social Security Administration Act 1999* (Admin Act)
*Disability Services Act 1986* (DSA)

## Learning Centre

Information Exchange and Privacy course (for DES)

## Explanatory Note:

All capitalised terms have the same meaning as in Disability Employment Services Grant Agreement.
In this document, "must" means that compliance is mandatory and "should" means that compliance represents best practice.

## 1. The Australian Privacy Principles

The Australian Privacy Principles (APPs) set out in Schedule 1 of the Privacy Act are principle-based laws that govern the way 'personal information' (including 'sensitive information') must be handled.

'Personal information' means information or opinion about an identified individual or an individual who is reasonably identifiable. The information or opinion does not have to be true and does not have to be recorded in material form.

'Sensitive information' is a subset of 'personal information' and is subject to a higher level of protection under the Privacy Act because its misuse could have greater adverse consequences for the individual concerned. 'Sensitive information' is information regarding certain characteristics of an individual, as specified in section 6(1) of the Privacy Act.

A flexible approach to implementing the APPs is encouraged, however compliance is mandatory.

The APPs should be embedded in daily operations. For example, DES Providers should regularly and openly discuss with Participants how their personal (including sensitive) information is being handled. Providers are encouraged to tailor their privacy practices to suit the needs of Participants and their own businesses whilst also meeting their privacy obligations.

Failure to comply with the APPs is considered to be an interference with the privacy of a Participant. A Participant who considers that their privacy has been interfered with can contact the Department to make a complaint. Alternatively, they can contact the Office of the Australian Information Commissioner who has powers to investigate possible interferences with privacy, either following a complaint by a Participant, or on the Commissioner's own initiative. In some circumstances, compensation may be paid to a Participant whose privacy has been breached.

For more information on the APPs refer to the Office of the Australian Information Commissioner's quick reference tool.

## 2. Notifiable Data Breaches (NDB) Scheme

All Providers with personal information security obligations under the Privacy Act must also comply with the requirements of the Notifiable Data Breaches Scheme2 when dealing with breaches of privacy.

Each breach of privacy must be assessed promptly in accordance with the requirements of the NDB scheme to determine whether an 'eligible data breach' has occurred and, if required, notification is to be provided to affected Participants and to the Office of the Australian Information Commissioner.

The Disability Employment Services Grant Agreement (the Agreement) under which Providers operate requires immediate notification to be made to the Department about any unauthorised access to, or disclosure of, personal information, or a loss of personal information the Provider holds. This applies to all breach incidents, whether or not they are an 'eligible data breach' for the purposes of the NDB scheme.

Details about the NDB scheme are available from the Office of the Australian Information Commissioner website.

## 3. Reporting unauthorised access, disclosure or loss of personal participant information

Providers must report all incidents involving unauthorised access, disclosure or loss of personal participant information to the Department as follows:

[2] Commenced on 22 February 2018

- notify your Relationship Manager/Funding Arrangement Manager using the Provider Incident Report on the provider Portal no later than the Business Day after the incident.
- prepare a detailed report of the incident, including details as appropriate to the incident (e.g.details of any potential breaches of privacy obligations etc.).
- forward this detailed report to your Relationship Manager/Funding Arrangement Manager as soon as possible and in any case within 15 business days of the incident.

Further details on your obligations for privacy breach reporting and record keeping can be found in the DES Record Management Instructions in these Guidelines.

---

## 4. Requests for access to or correction of a Participant's personal information

Under APP 12, individuals have a statutory right to request access to or correction of their own personal information held by their Provider. If a Provider receives a request under APP 12, they generally must process that request in accordance with the Privacy Act.

If a DES participant is seeking access to their personal information, DES Providers are required to comply with the DES Grant Agreement which states the Provider must allow Participants access to records that contain their personal information and provide them with copies of these records if requested by the Participant.

In accordance with the DES Grant Agreement, 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 Participant, or where it is clear that the Participant has a copy or has previously sighted a copy of the records)
- psychological records
- information provided by other third parties.

If the Provider has other particular concerns about the documents (for example, because they are sensitive in nature), they should refer the request to the Department to consider.

If someone is seeking access to personal information on behalf of another Participant, Providers must obtain written authority from the Participant whose personal information is being sought before releasing any documents. If the Provider is unable to obtain written authority, they should direct the individual to submit a formal Freedom of Information request to the Department of Social Services Freedom of Information team at foi@dss.gov.au.

---

## 5. Referring Participants to the Department in relation to privacy matters

Generally, requests or complaints under the Privacy Act should be directed to a Participant's Provider where possible. However, a Participant 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.

For general employment service matters, Participants should be provided with the following privacy contact details for the Department, on request:

By post: DSS Feedback
GPO Box 9820
Canberra ACT 2601

By email: complaints@dss.gov.au

By telephone: 1800 634 035.

For further information refer to the Department of Social Services Privacy Policy.

## 6. Notifying a Participant of Provider privacy requirements and seeking consent

During the initial interview or initial appointment, the DES Provider must ensure Participants are aware of the types of personal information they may be required to provide and how this information will be handled. Information is collected for the Department and the Provider to provide Participants with appropriate employment services and support, including:

- delivering employment services and help to find a job; or assisting in preparation for employment
- helping to evaluate and monitor the programs and services provided by the Department and its contracted Providers
- contacting Participants about their participation in the Department's programs and, where applicable, their mutual obligation or compulsory participation requirements
- helping to resolve complaints made by Participants or Providers
- involving Participants in surveys conducted by the Department or on behalf of the Department.

During the initial interview or initial appointment, the DES Provider must also seek the Participant's consent to collect and use their sensitive information by asking the Participant to sign the relevant DES Privacy Notification and Consent Form on the Provider Portal.

If the Participant refuses to sign the DES Privacy Notification and Consent Form this may limit the number of options and types of services the Provider can offer. The Participant should be made aware of this at the initial interview or initial appointment.

*[DES Grant Agreement 2018 clause reference: 41. (Personal and Protected Information) and 92. (Initial Interviews)]*

## 7. Participant privacy requirements when conducting the Job Seeker Classification Instrument (JSCI)

The JSCI measures a Participant's relative level of labour market disadvantage.

Information collected in the JSCI is personal (including sensitive) information under the Privacy Act. The DES Privacy Notification and Consent Form outlines how this information is collected, held, used and disclosed in accordance with the Privacy Act.

When conducting the JSCI, Providers must:

- notify the Participant and obtain consent for the collection of personal (including sensitive) information
- advise that the information provided is protected by the Privacy Act
- obtain consent for the collection of sensitive 'personal information' collected in the process of conducting the JSCI
- ensure they comply with the Privacy Act at all times.

💻 **System step:** The JSCI Change of Circumstances screen in the IT system includes a Privacy Statement that should be provided to or read to the Participant each time the JSCI is conducted.

🗐 **Documentary evidence**: Best practice is for Providers to ask the Participant to sign the relevant DES Privacy Notification and Consent Form available on the provider portal when:

- the JSCI is conducted
- the JSCI Change of Circumstances Reassessment is conducted

- where new personal (including sensitive) information is being collected, or
- it has been a long time since the consent was last provided to and signed by the Participant.

🗐 **Documentary evidence**: Consent can be given verbally or in writing. Where the Participant provides written consent, the signed copy must be retained on file.

💻 **System step:** If verbal consent is given for the collection of sensitive information, the Provider should make a record of the verbal agreement in the Participant's record in ESSWeb in the job seeker comments section.

More information on Assessments (JSCI and ESAt) can be found in the relevant programs' assessments guideline.

*DES Grant Agreement 2018 clause reference: 41 (Personal and Protected Information) and 120 (Change of Circumstances Reassessment during Period of Service)*

---

## 8. Releasing the Employment Services Assessment (ESAt) report

An ESAt is used by Services Australia to identify if a Participant has multiple or complex barriers to employment and may require more intensive support.

The ESAt report may be released to a Participant except where it contains information that may be prejudicial to the health of the Participant 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 Participant requests an ESAt report that contains the above statement, the Participant should contact the Department's Freedom of Information team at foi@dss.gov.au.

---

## 9. Privacy Requirements when sharing information with third parties

When referring Participants to Activities, employment opportunities or Host Organisations, Providers may need to share personal information about the Participant with a third party organisation. It is important that all Provider staff are aware of their obligations in relation to the disclosure of another Participant's personal information.

Providers are encouraged to regularly review and discuss privacy matters with the Participant, obtaining explicit written consent to the collection, use and disclosure wherever possible to ensure compliance with their privacy obligations.

It is important that Provider staff receive privacy training as Providers who conduct the checks /or have access to the results need to be aware of their privacy obligations. (Refer to mandatory annual DES privacy training below.)

**Note**: Participants under the age of 18 are permitted to sign the DES Privacy Notification and Consent Form as long as they do not have a guardian or administrator appointed. If appointed, the guardian or administrator should sign the DES Privacy Notification and Consent Form.

---

## 10. Privacy implications when conducting 'checks' and sharing information with a third party

If a Participant is offered paid work (either part or full-time) the Employer may seek a police/Working with Children check or require disclosure of the Participant's health/medical information. The Employer should be responsible for sourcing the checks and should seek the health/medical information directly from the Participant.

In all other instances the Provider should refer Participants to a third party and may need to arrange for 'checks' to be undertaken prior to placement. 'Checks' refers to police checks, Working with Children checks, Working with Vulnerable People checks, and Visa Entitlement Verification Online (VEVO) checks.

The Provider can choose an organisation to process police checks, however Working with Children or Vulnerable People checks will be processed by the relevant state or territory authority. A VEVO check will be processed on the Department of Home Affairs website.

The Provider must comply with relevant legal obligations in their respective state or territory to ensure Participants and/or supervisors have the appropriate checks in place prior to commencing the Participant in an Activity. Refer to the relevant program's activity management or participation guideline for information on what checks are required for an Activity.

A check form may include an 'Applicant's Consent' or an 'Applicant's Declaration' which will allow the information from a check to be given to a Provider. The information in the check will need to be taken into account when determining the Participant's suitability for placement in an Activity.

The Provider must ensure the Participant understands why the check is being undertaken, what information will be collected, and how that information will be used.

The Provider must not disclose the Participant's information to other parties unless consent is obtained using the relevant DES Privacy Notification and Consent Form to ensure the Participant understands what type of information is being released, for what purpose and to which parties.

The results of checks should be treated as sensitive information, and be handled in accordance with the Records Management Instructions of the relevant Grant Agreement, the Department's Security Policies, and any Privacy Act obligations.

If the Participant and/or supervisor request a copy of the results of their check, the Provider must ensure the Participant and/or supervisor provides proof of identity before they are provided with a copy.

*[DES Grant Agreement 2018 clause reference: 16 (Criminal Records Checks and other measures), 41 (Personal and Protected Information), 44 (Records the Provider must keep), 45 (Access by Participants and Employers to Records held by the Provider) and 100 (Safety and Supervision)]*

---

## 11. Disclosing the result of a police check to a third party

Before commencing a Participant in a placement with a third party, the Provider must ensure required police checks have been finalised. The third party will advise the Provider if the placement requires Participant to have checks completed for the paid work or Activity.

If a police check of a Participant indicates an offence that has a direct bearing on the placement, the Provider may be under a duty of care to the Host Organisation and have a legal obligation to disclose this, even where the police check was not required by the Host Organisation. Rather than disclose sensitive, personal information, in these instances, the Provider must consider another placement.

Where there is no legal requirement or obligation to disclose the information to the Host Organisation the results of the police check must not be disclosed.

If the Participant's police check indicates an offence that is not relevant to the Activity/place/course (e.g. driving related offences, where driving is not part of the Activity/course) the Provider needs to decide the best course of action for the Participant.

It should be noted even where a particular criminal record may not appear to be directly relevant to an Activity, it may be indirectly relevant. For example, numerous recent drink driving offences may be relevant where no driving is required as part of the Activity, if they are indicative of a drinking problem and part of the Activity/course requires the safe operation of dangerous machinery.

In these circumstances, the Provider needs to consider the results of the check and use careful judgment to decide the best course of action for the Participant, subject to any overriding legal obligations, such as the existence of a duty of care. Unless there is a specific legal obligation to disclose the results of the check, a Provider can generally only disclose the information to the Host Organisation with the Participant's consent. If the Host Organisation then reasonably decides it cannot accommodate that Participant in the placement, the Provider should seek another placement that does not require a check and complies with any Court ordered restrictions, or with a Host Organisation that will accommodate the Participant.

*[DES Grant Agreement clause reference: 16 (Criminal Records Checks and other measures) and 41 (Personal and Protected Information)]*

---

## 12. Managing the privacy implications when sharing a Participant's 'sensitive information' with third parties

Certain information regarding a Participant is 'sensitive information' for the purposes of the Privacy Act and should be handled carefully and afforded a greater level of protection from unnecessary disclosure to third parties.

'Sensitive information' includes the Participant's criminal history, religious beliefs, race, and medical history/issues. For example, the results of a police check may contain sensitive information about a Participant's criminal convictions and/or any time served in prison.

Under the Privacy Act, sensitive information can only be disclosed for the purpose it was collected unless an exception applies, such as where the Participant has consented or it is required or authorised by law. That is, where information in a check is obtained for the purpose of undertaking paid employment or a placement with a Host Organisation, then it is within the primary purpose to disclose the results to the Employer/Host Organisation so that the Participant can undertake that employment or placement.

The disclosure of sensitive information in checks may be authorised or required by law, or in circumstances where a duty of care arises. Determining whether a duty of care exists must be assessed on a case by case basis and it may be necessary to seek legal and/or other professional advice in this regard.

It may be necessary for the Provider to consider whether there is a duty of care such that the Participant:

- should not be referred to that Host Organisation as a result of the sensitive information, or
- may only be referred to that Host Organisation if the sensitive information is disclosed (for example, for the health and safety of other persons).

If the Provider determines that a duty of care exists, the following principles should be taken into account in deciding whether to share a Participant's sensitive information:

- the currency, accuracy and reliability of the information and the relevance of the information to the proposed placement
- whether the Host Organisation needs to know the information (e.g. does the information indicate a risk to the Participant or others?)
- whether the disclosure is relevant to the servicing of the Participant
- whether the information is relevant to the placement.

That is:

- Is there a duty of care such that the Participant should not be referred to that Host Organisation as a result of the sensitive information? or,
- Is there a duty of care such that the Participant may only be referred to that Host Organisation if the sensitive information is disclosed (for example, for the health and safety of other persons)?

Wherever possible, disclosing sensitive information to a third party should be discussed with the Participant to clarify what information, if any, they are comfortable to give their consent to disclose. This discussion should take place at the same time the Participant is requested to sign the relevant DES Privacy Consent Form and a record of the conversation should be retained.

---

## 13. Disclosing a Participant's medical information to a third party

Any health or medical information relating to a Participant will also be sensitive information and should be handled carefully to prevent unauthorised disclosure to a third party in relation to a placement.

When a Provider is aware of a health or medical issue the Participant has disclosed, this should always be considered in making referrals. This is because, amongst other things, the health of the Participant could be affected or exacerbated by the placement.

In these circumstances, the Provider should consider, subject to the Participant's consent, passing on the information to the relevant third party. The Provider should discuss the information with the third party to determine whether the Participant can be accommodated and whether the placement will be suitable. If the Provider, in conjunction with the third party decides the place is not suitable or they cannot mitigate the associated risk, the Provider should seek another suitable placement that does not pose a health risk to the Participant.

| |
|---|
| Example 1 – The Provider has organised four weeks of unpaid observational work experience in a bakery, however the Participant has advised they have a mild nut allergy. Following a risk assessment and consultation with the Host Organisation, it is agreed the Participant will undertake the placement but steps will be taken to ensure the Participant is protected appropriately and suitable medical contingencies will be put in place. |

*[DES Grant Agreement 2018 clause reference: 41 (Personal and Protected Information)]*

**Personal Information is directly relevant to a placement.**

| |
|---|
| Example 2 – The Provider organises a placement e.g. Voluntary Work with their Host Organisation in local parkland which is close to a school.<br><br>The Working with Children and police check indicates that the Participant has convictions which preclude him/her from being within 100 metres of a school.<br><br>The Provider finds another placement not close to schools or other organisations involving children in order to ensure the Participant complies with his/her Court ordered agreement/restrictions. |

**Personal information is not directly relevant to a placement.**

| |
|---|
| Example 3 – A Provider identifies a placement at a school canteen. The Host Organisation requests a Working with Children check as required by legislation. The Provider applies for a Working with Children check (which includes a police check).<br><br>The Working with Children check indicates that the Participant is permitted to work with children but discloses a recent Driving Under the Influence charge. After conducting the required Risk Assessments (place and Participant), the Provider is satisfied that the results of the police check are not relevant to the Participant's ability to safely carry out the activity.<br><br>In this case, the personal information would not be required to be disclosed to the Host Organisation.<br><br>The Provider needs to consider each case on its merits as to whether the check is relevant and should be passed to the Host Organisation. Results of checks must not be passed to Host Organisations in all cases. |

*[DES Grant Agreement 2018 clause reference: 41 (Personal and Protected Information) and 44 (Records the Provider must keep)]*

---

## 14. Releasing protected information to a third party (including the police) using a Public Interest Certificate

Information held about Participants may be governed by both the Privacy Act and social security law. Importantly the same piece of information may be both personal information under the Privacy Act and protected information under social security law. For example, the name and contact details of a Participant

who receives a social security benefit or payment, will likely be both personal and protected information, disclosure of which will be governed by both social security law and privacy law.

Certain provisions in social security law enable the disclosure of protected information in particular circumstances. Section 208 of the *Social Security (Administration) Act 1999* makes provision for the Secretary of the Department of Social Services to allow use or disclosure of protected information by issuing a Public Interest Certificate (PIC).

Additionally, information held about DES participants may also be governed by the *Disability Services Act 1986* (Disability Services Act) in addition to the Privacy Act and social security law. Information acquired in the performance of duties or exercise of powers in relation to the provision of rehabilitation services by the Commonwealth under the Disability Services Act is protected information. Section 28 of the Disability Services Act makes provision for the Secretary of the Department of Social Services to allow use or disclosure of protected information by issuing a PIC.

A PIC identifies the information that can be released about a DES Participant; who it can be released to; who can release the information; and allows the information to be released.

Except in the specific circumstances described in the Class PIC below, Providers will need to approach the Department through their Relationship Manager/Funding Arrangement Manager to arrange a PIC from the Department of Social Services to cover the release of protected information as soon as they become aware of a circumstance where they wish to, or are being asked to, disclose protected information.

### Class PIC for DES Providers

The Secretary of the Department of Social Services has issued a Class PIC that authorises DES Providers to disclose protected information only where there is a threat to someone's life, health or welfare (Threats).

In the case of Threats, the protected information can only be released to: emergency services (including the police); health service Providers; and child protection agencies.

Once the Provider's site manager or more senior manager has released the information, the Provider must notify their Relationship Manager/ Funding Arrangement Manager using the Release of Protected Information Notification Form on the Provider Portal.

**Only people who are appropriately authorised by the PIC** can release protected information. For more information on who has authority and the requirements around releasing protected information under the Class PIC please refer to **the DES Class PIC Factsheet** on the Provider Portal.

Providers are required to obtain a separate PIC for situations that are not covered by the Class PIC.

*[DES Grant Agreement clause reference: 44 (Records the Provider must keep) and 41 (Personal and Protected Information)]*

---

## 15. Mandatory Annual DES Privacy Training

The Department has developed a range of resources to assist Providers to comply with their obligations under the Agreement, the Privacy Act 1988 (Cth) (Privacy Act) including the Australian Privacy Principles (APPs), and relevant social security law. One of the resources is the Information Exchange and Privacy Course (for DES) (DES privacy Course), available on the Learning Centre. This course outlines the obligations of Provider Personnel under the Privacy Act. The department also recognises that most Providers have their own privacy training arrangements in place.

In addition to these arrangements, and in recognition of ongoing and emerging privacy risks and impacts, the department is taking steps to further strengthen safeguards in place to secure personal information from misuse, interference or loss, or from unauthorised access, modification or disclosure.
Pursuant to clause 53.3 of the Agreement, the Department directs your organisation to ensure that all Personnel who handle personal information in the course of delivering Services under the Agreement have completed, at a minimum, the DES privacy Course on the Learning Centre:

(a) prior to delivering the Services; and

(b) thereafter at least once in every subsequent 12 months.

Provider personnel who have not completed this updated mandatory annual DES privacy course through the online Learning Centre by 11 October 2022 will be blocked from accessing the Department's system. The user will be presented with a page informing them they must complete the mandatory DES privacy training in order to gain access.

It can take up to four hours before ESSWeb is aware the user has completed the mandatory DES privacy course. The Learning Centre has advised this timeframe cannot be altered.

Providers are required to complete the Information Exchange and Privacy course (for DES) once in every subsequent 12 months.