Australian Government

Guideline:

Records Management Instructions

The Records Management Instructions (RMI) provide legally binding instructions on the management, retention and disposal of identified 'Records' created or used by organisations contracted to deliver employment services by the Department of Education, Skills and Employment (the Department) under one or more of its Deeds (Providers).

The RMI is a Guideline for the purposes of the Deeds and applies to any Deed or contract administered by the Department that refers to the RMI.

Version: 2.4

Published on: 28 February 2022

Effective from: 28 February 2022

Changes from the previous version 2.3

Policy changes:

Nil

Wording changes:

- Updated links to National Archives of Australia website

A full document history is available in the Archived Guidelines section on the Contractual Information page.

Related documents and references

- General Records Authority (31) Destruction of source or original records after digitisation, conversion or migration
- Employment Services Records Authority, including retention periods of different Records
- General advice on the management and storage of digital records
- General Records Authority 33 Accredited Training
- Privacy Guideline
- The Office of the Australian Information Commissioner Guide to securing personal information

Contents

1 Records Framework

Providers must create and maintain true, complete and accurate Records of the conduct of their services, and do so in accordance with these Records Management Instructions.

Under the relevant Deeds, '**Records'** means documents, information and data stored by any means and all copies and extracts of the same. Records can generally be separated into three groups:

- **Commonwealth Records** – which means Records provided by the Department to Providers for the purposes of the relevant Deed and includes Records which are copied or derived from Records so provided.
- **Deed Records** – which means all Records:
    - developed or created or required to be developed or created as part of or for the purpose of performing the relevant Deed;
    - incorporated in, supplied or required to be supplied along with the Records referred to in paragraph (a) above; or
    - copied or derived from Records referred to in paragraphs (a) or (b); and
    - includes all Reports.
- **Provider Records** – which means all Records, except Commonwealth Records, in existence prior to the relevant Deed Commencement Date:
    - incorporated in;
    - supplied with, or as part of; or
    - required to be supplied with, or as part of the Deed Records.

2 Deed Records

2.1 Requirements

Providers may create Records in either paper or digital form. Arrangements outlined in this RMI cover both forms of a Record. Consistent with the Department's recordkeeping policy, it is preferred that all Records are created and managed digitally.

Records may be created digitally provided the requirements of the *Electronic Transactions Act 1999 (Cth)* and the relevant Deed are met. Subject to Section 3, Providers can retain Records in a manner that suits their own business arrangements.

Commonwealth Records, as defined in section 1 above, are 'Commonwealth Records' for the purposes of the *Archives Act 1983* (Archives Act). Subject to certain exclusions and conditions, the National Archives of Australia (NAA) provides permission for the destruction of Commonwealth Records created on or after 1 January 1980 under General Records Authority 31 (GRA 31) where those Records have been converted from hard copy to digital form. GRA 31 applies to Providers as 'authorised agents' of the Department. Providers must comply with the requirements of GRA 31. For convenience, the relevant exclusions and conditions are set out below.

2.1.1 GRA 31 Exclusions

GRA 31 does not cover the destruction of Records that have been reproduced where:

- The Records identified for permanent retention ('retain as national archives (RNA)' or 'retain permanently (RP)') and have special or intrinsic value in the original medium which would be lost if the content were converted to another medium.
- The Records subject to specific legal or administrative requirements such as:
  - legislation that requires retention of the original or source Record in a specified form; or
  - a government policy or directive not to destroy the original or source Record.
- The digital original or source Records converted to paper or another physical format.

2.1.2 GRA 31 Conditions

- Source records which were created before 1 January 1980 and which have been identified for permanent retention (RNA or RP) may not be destroyed without specific approval from the National Archives. These will be considered on a case-by-case basis.
- Providers must consider the risks and may need to seek legal advice and permission from the Department before destroying source or original Records which are subject to specific legal or administrative requirements such as:
  - Those that are likely to be required as evidence in a current judicial proceeding or a judicial proceeding that is likely to commence; or
  - Those that are the subject of a current application for access under the *Freedom of Information Act 1982*, *Archives Act 1983* or other legislation.
- In general, this authority may be applied to source or original Records subject to a disposal freeze or retention notice provided the terms of the disposal freeze or retention notice do not specifically exclude application of this authority.
- Providers must ensure all copies or reproductions that have been created as a result of digitisation, conversion or migration are at least functionally equivalent to the source or original records for business, legal and archival purposes.
- Functional equivalence means that copies or reproductions have the same degree of authenticity, integrity, reliability and usability as the source or original Records.
- Source or original Records must be kept long enough to complete quality control processes on the copies or reproductions.
- Digitisation processes must meet National Archives standards, specifications and guidelines. This includes scanning specifications for paper Records that have been digitised and technical specifications for digitising audio visual Records.
- Providers must maintain digital information in accordance with National Archives' standards and guidelines and retain information and Records according to the relevant records authority.
- The creation date of the source or original Record is to be used as the creation date of the copy or reproduction for the purposes of the Archives Act.

Further explanation of the relevant exclusions and conditions is provided at General Records Authority (GRA) 31 on the National Archives of Australia Website (at http://www.naa.gov.au/information-management/records-authorities/types-of-

records-authorities/GRA/GRA31/index.aspx). Providers must have regard to this authority in developing any practices and policies for converting paper-based Records into digital format and, after doing so, in relation to the destruction of the original paper-based Records.

Records scanned into a digital system must also be retained in accordance with this RMI, and in particular any relevant retention periods.

Information in the Department's IT Systems will be retained by the Department for the appropriate retention periods.

Refer to Section 7: Return of Records for more information on digital Records.

NOTE: Providers **must** retain the original copy of a paper Record for the relevant retention period, regardless of whether it has also been converted to digital form, if required to do so under relevant program Guidelines or if directed by the Department.

3 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.

3.1 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/Deed Records, for example, the *Privacy Act 1988 (Cth).* At Australian Privacy Principle 11, the *Privacy Act 1988 (Cth)* requires entities to take active measures to ensure the security of Personal Information they hold. In addition, Providers are required to store Records in accordance with the Department's Security Policies (including the Security Policy For External Employment Services Providers and Users (available on the Provider Portal or via the Department's website (at www.dese.gov.au). The Guide to securing personal information can be found on the Office of the Australian Information Commissioner website (at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information) and provides guidance on the reasonable steps entities are required to take under the *Privacy Act 1988 (Cth)* to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure.

Providers must ensure that the Department has access to Records if required, either by providing access to a storage facility or by retrieving the Record (including if stored digitally by retrieving the digital copy and if relevant printing it) and providing it to the Department.

Providers must ensure Records are protected from:

- storage environment damage (e.g. for paper Records, damp from a cement floor and protected from fire);
- unauthorised alteration or removal;
- use outside the terms of the relevant Deed;
- for Records containing Personal Information, incidents of privacy; and

- inappropriate 'browsing' of Records by Provider staff or any other person.

Records containing sensitive information as defined in the *Privacy Act 1988 (Cth)*, such as criminal records or health information about an individual, must be kept in lockable cabinets or (if digital) on a secure information system.

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

3.2 Digital Record Storage Requirements

Providers that choose to store Records digitally must ensure all Record storage systems operate in accordance with the storage and physical access requirements outlined in this RMI, the relevant Deed and the Department's Security Policies. An assessment of any potential risks must be undertaken prior to storing Australian Government Records in data centres, digital repositories and the cloud.

Where Providers migrate digital Records to a new storage device or system, or change the file format of a digital Record to the extent that it is relevant, Providers must comply with GRA 31 in destroying the source Record (i.e. the original digital Record). Refer to Section 2: Deed Records for more information on GRA 31.

General advice on the management and storage of digital Records is available on the National Archives of Australia website.

Providers should note that they must not:

- give Access to digital Records relating to the services or any derivative thereof, to any Third Party IT Provider who has not entered into a Third Party IT Provider Deed with the Department and only grant such Access in accordance with the terms of the Third Party IT Provider Deed and any Guidelines. Providers should refer to their Deed for details of those obligations; or
- transfer relevant Personal Information outside of Australia, or allow parties outside Australia to have access to it, without the prior written approval of the Department.

3.3 Unauthorised Access, Damaged, Destroyed, Lost or Stolen Records

3.3.1 Reporting Requirements

Note: Reporting requirements for Third Party IT Providers are contained in the Third Party IT Provider Deed (at https://www.dese.gov.au/employment-services-purchasing-information/resources/department-employment-third-party-it-provider-deed). Third Party IT Providers must also comply with section *3.4.3 - Notifiable Data Breaches Scheme.*

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

- notify the relevant Account Manager or Departmental employee using Part 1 of Attachment A: Provider Privacy Incident Report no later than the Business Day after the incident;
- report any incidents involving stolen Records to the police immediately; and
- prepare a detailed report of the incident using Part 2 of Attachment A: Provider Privacy Incident Report, including details as appropriate to the incident and submit this detailed report to the Account Manager as soon as possible and, in any case, within 30 calendar days of the incident. **NB:** If this report cannot be

submitted within 30 days, advice must be provided to the Department explaining the delay.

3.3.2 Rectification Requirements

For all incidents involving unauthorised access, damaged, destroyed, lost or stolen Records, Providers must:

- immediately make every effort to recover lost or damaged Records (e.g. retrieving or photocopying Records), including if required, arranging and paying for the services of expert contractors (e.g. disaster recovery or professional drying services);
- not destroy damaged Records without authorisation from the Department
- inform Participants if any Personal Information has been lost or is at risk of being publicly available;
- where relevant and, if necessary, reinterview Participants to recollect information; and
- review relevant policies and procedures to ensure their adequacy in future. The Department may make recommendations to the Provider to mitigate the risk of recurrence of the incident.

3.3.3 Notifiable Data Breaches Scheme

All providers, and the organisations or agencies they share information with, must comply with the requirements of the Notifiable Data Breaches (NDB) scheme (at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme) in the event of an 'eligible data breach' involving personal information.

Under the NDB scheme, Providers who become aware of an incident involving personal information must undertake a reasonable and prompt assessment and investigation. The Provider should consider whether the incident is an 'eligible data breach', and then notify affected individuals and the Office of the Australian Information Commissioner (OAIC) where an 'eligible data breach' is found to have occurred. The Department must also be informed of the incident in accordance with section 3.3.1-Reporting Requirements and provided with copies of any notifications.

Further information about the NDB scheme and guidance for undertaking an assessment of a privacy incident (to determine whether it is considered an 'eligible data breach), is available from the OAIC website (at http://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme).

The NDB scheme does not vary the obligation of Providers to immediately notify the Department and manage any actual or suspected breach of privacy involving personal information. This includes notifying the Department of privacy incidents that do not qualify as an eligible data breach under the NDB scheme. See section 3.3.1 for Reporting Requirements.

4 Control of Records

Where Providers hold Records about a Participant, Providers must be able to locate and retrieve such Records if requested.

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

4.1 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 a digital format (ideally Microsoft Excel or equivalent or a comma or tab limited format) that the Department's IT system can read.

To the extent Providers are in possession of the following Records, 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; or
- Returned – Records have been returned to the Department.

For the purposes of the RMI, 'inactive Records' means Records created under previous contractual arrangements.

Examples of priority Records include Records documenting:

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

Refer to Section 6: Records Retention for information on the retention of the Records list.

5 Transfer of Records

5.1 Transfers between Providers [1]

Records must only be transferred between Providers under the relevant Deed if this is required to continue providing Services to Participants in accordance with the relevant Deed. 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 4.1: Control of Records – Records List) being transferred should be provided to the receiving Provider.

The transfer of Records containing Personal Information and Protected Information must be in accordance with the *Privacy Act 1988 (Cth)* and the *Social Security (Administration) Act 1999* respectively.

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.

[1] Note: Section 5.1 is not applicable for all Providers. Each Deed will outline whether Records are required to be transferred between Providers.

5.2 Transfer of Personal Information outside Australia

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

6 Records Retention

Providers must retain relevant Records according to the minimum retention periods outlined in Attachment C: Records Retention Periods. Where a Record is not covered by Attachment C, Providers must retain that Record in accordance with the relevant Deed.

Where a Third Party IT Provider is in possession of Records identified in Attachment C as a result of assisting a Provider to provide Services to the Department under the relevant Deed, the Third Party IT Provider may only dispose of those Records in accordance with Attachment C where it has the prior agreement of the relevant Provider.

Providers must review relevant Records that have reached the minimum retention period before destroying in accordance with the RMI. If a relevant Record has reached the required minimum retention period but, for example, the Provider has knowledge of a legal action or potential legal action, the Provider must re-sentence[2] the Record and must inform the Account Manager.

Retention periods apply to all formats of relevant Records whether created in paper or digitally 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. For more information regarding this, please refer to Section 2.1.2: Deed Records – Requirements – Conditions.

Refer to Section 8: Destruction of Records for more information on destroying Records.

7 Return of Records

If requested, Records must be returned to the Department within 28 Business Days unless otherwise specified by the Department.

Providers must obtain the Department's approval prior to returning any Records to the Department. Providers may seek permission to return Records to the Department following the Completion Date and should do so by completing Attachment B: Provider Request to Return Records and submitting to their Account Manager. Please note that the request must be accompanied by a list of the Records the Provider is requesting to return.

Refer to Section 4.1: Control of Records – Records List for information on list requirements.

[2] Sentencing is the process for identifying the minimum retention period for a Record by assessing them against the classes specified in the relevant records authority.

Providers under a relevant Deed who had a previous 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 the relevant time (e.g. under the Records Management Instructions for the Employment Services Deed 2009-2015). Records of Participants continuing to receive Services are required to be managed in accordance with the relevant Deed and this RMI.

The Department's preferred format for Records to be returned is digitally in a common readable format e.g. in a single scanned PDF format. Providers must ensure digital Records transferred to the Department are readable, identifiable and are not corrupted. Documents must have meaningful titles and be contained within a single Participant folder listing the Job Seeker Identification (JSID), first name and last name (e.g. JSID 1234 SMITH, JOE).

7.1 Digital Records

Providers creating digital Records must use a format that is acceptable under the Archives Act and that will allow the Department to read the Records if returned to the Department in the future. As such, the Department requests that digital Records be created and managed in Microsoft Office (or the open source equivalent) formats, or in PDF format. If the Provider elects not to use these formats, then Records will need to be converted into either one of these formats before being returned to the Department.

Digital Records contained on the Department's IT Systems or created for purposes other than in accordance with the Deed do not need to be returned.

7.2 Access to Returned Records

Where Records have been returned to the Department and a Provider requires access to those Records, the Provider must write to the Account 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* (Cth).

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, it is advisable for the Provider to contact the Department. In these circumstances, the Provider should seek their own independent legal advice.

8 Destruction of Records

Providers must not destroy or dispose of Records other than in accordance with their relevant Deed, this RMI or as directed by the Department. When Providers destroy Records, they must use a method that ensures the information is no longer readable and cannot be retrieved.

Records must not be destroyed where Providers are aware of current or potential legal action even if the minimum retention period has been reached. These Records are priority Records and must be retained in accordance with requirements set out for priority Records in Section 4.1. A Provider must also comply with any direction from the Department not to destroy Records. Subject to Section 2: Deed Records,

Providers must only destroy Records that have reached the minimum retention period and following the review process outlined in Section 6: Records Retention.

Providers must maintain a list of destroyed Records which 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 4: Control of Records for more information on the tracking of Records and Section 6: Records Retention for more information on retention periods.

8.1 Methods of Destroying Physical Records

Providers must ensure physical Records are destroyed using one of the following methods:

- Pulping – transforming used paper into a moist, slightly cohering mass;
- Burning – in accordance with relevant environmental protection restrictions; and
- Shredding – using crosscut shredders (using either A or B class shredders).

If destruction of physical 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.

8.2 Methods of Destroying Digital Records

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

Methods of destroying digital Records include:

- digital file shredding;
- degaussing – the process of demagnetising magnetic media to erase recorded data;
- physical destruction of storage media – such as pulverisation, incineration or shredding; and
- reformatting – if it can be guaranteed the process cannot be reversed.

To ensure the complete destruction of a digital Record, all copies should be found and destroyed. This includes removing and destroying copies contained in system backups and off-site storage.

All capitalised terms in this guideline have the same meaning as in all Deeds.

In this document, 'must' means that compliance is mandatory and 'should' means that compliance represents best practice for Relevant Providers.

This Guideline is not a stand-alone document and does not contain the entirety of Providers' obligations. It must be read in conjunction with the Deed and any relevant Guidelines or reference material issued by the Department of Education, Skills, and Employment under or in connection with the Deed.

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 responses/s 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. 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**

Attachment B – Provider Request to Return Records

Australian Government
Department of Education, Skills and Employment

Provider Request to Return Records

Providers must complete this form before Records are returned to the Department of Education, Skills and Employment.

- Provider to complete Section 1 and submit to their Account Manager.
- Account Manager to complete Section 2 and forward to the Department's Information Management Team.
- Provider to liaise with Account Manager in relation to the progress of their request.

Section 1 – Provider to complete	
Provider legal name and ABN:	Contact person:
Provider address:	Phone number:
Total number of files:	Service(s):
Expected retention:	Time left on retention:
Reason for request to return:	
Section 2 – Account Manager/Department's Deed Manger to complete	
Name and phone number:	Date / /
Reason for return of Records:	
Section 3 – Records and Information Management to complete	
Name of Record Management Officer:	Date / /
Final action:	

A list of all Records the Provider is requesting to return must be attached to this pro forma, and must contain information as specified in Section 5.1: Control of Records – Records List.

Retention Periods

Records Authorities (RA)

The Employment Services Records Authority 2009/00179260 (RA) and the General Records Authority GRA 33 Accredited Training 2012/00579704 (GRA 33), 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 and GRA 33 provide the legislative framework for the destruction of Records following minimum retention periods as set out in the RMI.

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

Regardless of the disposal actions outlined under the RA, the Department may impose special conditions on Providers Records management at the Department's absolute discretion. This may include imposing extended record retention periods on Providers.

The Records description and examples below are intended to 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. For a full description of the categories of Records covered and their relevant retention periods please refer to the RA.

RA interpretation

In addition to the retention policy below, where there is potential for any legal action or as otherwise advised by the Department, Records must be retained for seven years after the matter is resolved.

- Any other Records as advised by the Department

Table 1: Employment Services Records Authority (RA) 2009/00179260 Participant Records

Entry	Description of Records as outlined under the RA	Includes but is not limited to	Disposal action
20184	Records documenting accidents or incidents to Participants engaged in employment services programs, including all relevant Records associated with that Participant.	• Incident/accident information • Potential legal action/fraud Records • Customer feedback register • Risk assessments • Other related documentation.	Destroy 6 years after last action [unless legal action or litigation is underway, in which case the Records must be retained for 7 years after the matter is resolved].
20186	'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.'	• Documentary Evidence as detailed in the Documentary Evidence Guidelines • Job Plans • Documentary Evidence as required to verify Job Seeker Classification Instruments • Activity agreements • Employment Fund Records • Training credits information • Proposed NEIS business plans • Monitoring/mentoring information • All placement information • Activity attendance records • Records relating to the provision of Services and support to Participants • Checks, such as police checks or working with vulnerable people checks • Activity Host Agreements • Other related documentation	Destroy 3 years after last action

Entry	Description of Records as outlined under the RA	Includes but is not limited to	Disposal action
20195	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.	• Documentary Evidence as detailed in the Documentary Evidence Guidelines • Job Plans • Documentary Evidence as required to verify Job Seeker Classification Instruments • Activity agreements • Employment Fund Records • Training credits information • Proposed NEIS business plans • Monitoring/mentoring information • All placement information • Activity attendance records • Records relating to the provision of Services and support to Participants • Checks, such as police checks or working with vulnerable people checks • Activity Host Agreements • Other related documentation	Destroy 3 years after last action

Entry	Description of Records as outlined under the RA	Includes but is not limited to	Disposal action
20199	Records documenting the provision of employment services	• Documentary Evidence as detailed in the Documentary Evidence Guidelines • Job Plans • Documentary Evidence as required to verify Job Seeker Classification Instruments • Activity agreements • Employment Fund Records • Training credits information • Proposed NEIS business plans • Monitoring/mentoring information • All placement information • Activity attendance records • Records relating to the provision of Services and support to Participants • Checks, such as police checks or working with vulnerable people checks • Activity Host Agreements • Other related documentation	Destroy 3 years after last action

Table 2: General Records Authority GRA 33 2012/00579704 Accredited Training Records

Entry	Description of Records as outlined under the RA	Disposal action
61248	Records documenting: • Registered Training Organisation's (RTO's) compliance with legislative and regulatory requirements and mandatory or optional standards. Includes accrediting body audit results, and records of breaches, grievances or appeals; • advice to regulatory bodies, such as that relating to changes to the structure or status of the RTO. Includes the discontinuance of, or significant changes relating to, an accredited training course; • evaluation of potential or existing training programs and services, including consultation with industry; • successful funding applications made by the RTO to federal, state or territory governments; • negotiation, establishment, maintenance and review of routine operational agreements relating to the RTO; • final versions of formal internal and external reports such as training statistical reports and self-assessment reports; • completed trainee assessment items such as written assignments, where there has been a grievance or appeal; and • enrolment of students into a training program or course, including enrolment forms and student identification documents and recognition of prior learning	Destroy 10 years after action completed
61249	Master set of training material for training and workshops run by the RTO: • programs • lecture notes • instructional materials • films and videos • online modules • supporting records	Destroy 3 years after training material is superseded
61250	Records documenting: • non-contractual administrative arrangements supporting the delivery of accredited training by the agency, including facility and trainer bookings, invitations, applications, reminders, confirmations, travel and catering arrangements; • completed trainee assessment items such as written assignments, where there has been no grievance or appeal; and • receiving and responding to low level general enquiries in relation to accredited training which require a routine/standard response, such as course enquiries.	Destroy 2 year after action completed