# DATA RETENTION AND DESTRUCTION POLICY

Last updated: April 2023.

|  |  |  |  |
| --- | --- | --- | --- |
| Policy number | <<insert number>> | Version | <<insert number>> |
| Drafted by | <<insert name>> | Approved by Board on | <<insert date>> |
| Responsible person | <<insert name>> | Scheduled review date | <<insert date>> |

This policy has been prepared for organisations that have obligations in relation to data retention under the Privacy Act as well as under other legislation. Does the Privacy Act apply to your organisation? Check the criteria [here](https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities#WhoHasResponsibilitiesUnderPrivacyAct). ]

# Background

(**[##Organisation]**) must comply with the the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs) and any other applicable privacy laws.

[##Organisation] also has legal obligations to keep certain kinds of data on record for a specified amount of time. The table in Appendix 1 sets out the legally required retention periods for common categories of data.

This policy sets out [##Organisation]’s approach to managing, retaining and destroying records and data (including personal information) we hold, to ensure compliance with the APPs and data retention laws. The purpose of this Policy is to outline roles, responsibilities, and steps [##Organisation] and staff must take when dealing with record and data retention and destruction.

This policy does not cover all circumstances that may arise, is not a comprehensive statement of the relevant law, and is not a substitute for legal advice. If you are unsure or have any questions about this policy, or [##Organisation]’s obligations, you should consult [Insert contact number, email address and name for person in charge of implementing this policy].

# Scope

## What do we mean by ‘record’ and ‘data’?

### The Privacy Act provides that a ‘record’ can be a paper document or an electronic file. Records may include physical documents, digital scans of documents, databases, and electronic files such as text, image, video, or audio files. In essence, any medium that captures and contains information constitutes a ‘record’.

### In this policy, ‘data’ means any information which is contained in a record, including (but not limited to) personal information.

## Who does this policy apply to?

* + 1. This Policy applies to all employees, including temporary employees, contractors, and volunteers who have access to [##Organisation] records and data or who are involved in the process of collecting, storing or securing [##Organisation] records and data on behalf of [##Organisation].

General rules and principles

## Information lifecycle

### The information lifecycle describes each phase of [##Organisation] records and data.

### This policy focuses on the ‘Hold’ and ‘Destroy’ phases. ‘Hold’ refers to how records and data are recorded, stored, secured, backed-up and archived, while ‘Destroy’ refers to how records and data are disposed of or put beyond use. For personal information, ‘Destroy’ also covers the de-identification of that information so that it is no longer considered personal information.

### The Privacy Act requires us to delete personal information when no longer required (which includes for any legal purpose), but data retention laws may require us to keep that personal information for certain periods of time. Privacy laws and data retention laws may appear to conflict but it is essential to consider both obligations together.

### You must consider and apply the guiding principles set out below when managing, retaining and destroying records and data.

## Guiding principles on managing, retaining and destroying records and data

### Actively and continuously consider whether retention of data is necessary.

### Do not destroy records and data that are necessary for [##Organisation]’s business functions or legally required to be kept.

### Do not destroy records and data that may be relevant to ongoing or anticipated disputes, litigation or regulatory investigations. Consult with [Insert contact number, email address and name for person in charge of implementing this policy] if you have doubts about whether certain records or data should be retained for their evidentiary value.

### **Retain only minimum data necessary.** It is possible to have too much data. Over-collection of data is a significant risk. Only keep what is reasonably necessary for [##Organisation]’s business functions or to comply with our legal obligations.

### **Consider whether** [##Organisation] has contractual obligations to destroy certain records and data after the expiration of a contractual relationship.

### **Record data in the most appropriate format and minimise paper records.** Scan physical documents and save the digital scans in [##insert name of document management system]. Do not use your email inbox as a record filing system.

### **Take steps to secure your records and data and minimise risk of corruption of data or accidental loss**. Ensure that important data is securely backed-up and archive records when they are not actively being used (but which are not ready to be destroyed).

### **Ensure data can be easily located and accessed** (even when archived or not in active use).

### **Ensure paper records are securely destroyed if appropriate**. Use shredders or security bins to destroy paper records.

# Steps to manage data

[***Drafting Note: Depending on the size of your Organisation and how data rich it is, the processes below may need to be adapted to suit your Organisation***]

## Step 1: Identify record, data and purpose

### Step 1 is to identify:

#### the data that you deal with and the records in which they are contained (i.e. certain data may be in multiple records)

#### the purpose for which the data was collected

#### the purpose for which the data (and record) is currently being held.

### The data and records that you deal with in your day-to-day activities will depend on your role. For example, an employee in our [##Human Resources / People and Culture department] may regularly collect and handle:

#### tax file numbers in records relating to employees

#### role and salary information

#### identification documents (records such as scanned passports and drivers’ licences)

#### contact information

#### health information

#### of our employees and contractors for payroll purposes and to comply with our legal obligations.

### An employee in our [Marketing / Business Development / Sales department], on the other hand, may regularly collect and handle customer:

#### email addresses

#### consents

#### preferences

#### cookie data

to promote our goods and services.

### To identify the kinds of data you handle, and what possible obligations may attach to them, ask yourself:

#### What data do I use to carry out my functions?

#### Does that data contain personal information about individuals?

## Step 2: Determine whether it is necessary to retain the data (and relevant records) and, if so, for how long.

### Data is sometimes collected for one-time use, and once the purpose for which it was collected is fulfilled, it is not necessary to retain it. In such circumstances, you should promptly delete or destroy the data (and relevant records), especially if it contains personal information about individuals, to minimise the risk of that data being compromised in the event of a data breach. This is particularly important in relation to government issued identifiers such as passport and drivers’ licence numbers.

### Certain data (and relevant records) must be retained because they are necessary for [##Organisation]’s business functions, or because the law requires that the data be retained for a specific period of time. If you determine that it is necessary to retain the data and record identified in Step 1, determine whether it falls into a category with a specific retention period (see Appendix 1). If so, you should take reasonable steps to ensure that the data is destroyed after that period has elapsed (see Step 4).

### If the data and relevant records do not fall into a specific category, but are required to be retained, best practice is to retain the data (and relevant record):

#### for seven years for financial and governance records;

#### for seven years if it is personal information about an adult

#### for seven years after a child turns 18 if it is personal information about a child

#### until it is no longer necessary for the purpose for which it was collected (whichever is the longer).

### Consult with [Insert contact number, email address and name for person in charge of implementing this policy] for advice on determining the appropriate retention period for records and data that do not fall into a category set out in Appendix 1.

## Step 3: Decide how, and in what format, the data should be held.

### If the data is recorded in hard copies (i.e. paper records), the general rule is that the document should be scanned and stored electronically, and that the physical paper copy should be securely destroyed. An exception applies to original versions of documents which are legally required to be retained (see Appendix 1) or which [##Organisation] may be required to produce as evidence in a dispute, legal proceedings or an investigation.

### Consider whether the data (and relevant records) will need to be regularly accessed or whether they should be archived. In either case, the data (and relevant records) should be held in a manner which allows them to be easily located, accessed and retrieved when needed. If you decide to archive the data, be sure to record the date the data was created, the date it was archived, and the date after which it should be destroyed.

### Data should be stored securely and in a manner that is appropriate to the value and sensitivity of the data, and the physical properties (if applicable) of the record (for example, paper records should be stored in a cool, dry place outside of direct sunlight to avoid degradation).

### As a general rule, email inboxes and mailbox folders should not be the primary source of storing records and data, particularly data which consists of personal information or sensitive information. File records with personal information, sensitive information, financial information or government identification numbers in [insert name of #Organisation’s document management system].

## Step 4: Determine whether and how the data should be destroyed, put beyond use, or de-identified.

### In most circumstances, data (and the relevant record) should be destroyed after its retention period has elapsed and it is no longer required for a business function or to comply with a legal requirement.

### There may be occasions where it is not possible or practicable to irretrievably destroy data (because, for example, the system on which the data is stored does not allow data to be deleted, or where the data is part of a larger dataset). These circumstances should be avoided if possible, but if they arise, you should take reasonable steps to:

#### put the data beyond use. The Office of the Australian Information Commissioner (OAIC) has said this means [##Organisation]:

##### is not able (and will not attempt) to use or disclose that data, and

##### cannot give any other entity access to that data, and

##### surrounds the data with appropriate technical, physical and organisational security. This should include at a minimum, access controls including logs and audit trails, and

##### commits to take reasonable steps to irretrievably destroy the data if, or when, this becomes possible; or

#### **de-identify the data**: If the data contains personal information or sensitive information, consider whether it is possible and practicable to de-identify the data. This means taking steps to remove information that could reasonably identify an individual (for example by redacting scanned documents).

### There may be certain circumstances in which the data should be de-identified immediately (such as where it is being used for analytics or research purposes, which does not require individuals to be personally identifiable.

# Roles and responsibilities

[***Amend below to reflect titles, roles and responsibilities in your organisation.***]

## Business units

### Determine retention periods for the records they hold, having regard to:

#### legally required retention periods (see Appendix 1)

#### whether the retention of the record or data is (and continues to be) necessary for one or more of [##Organisation]’s functions and activities

#### whether the record or data (and the relevant record) may hold evidentiary value in an existing or potential dispute, legal proceeding or regulatory investigation

#### the guiding principles set out in section 3.2.

### Ensure that records and data are securely held, and that appropriate roles, responsibilities, practices and processes are put in place to ensure that records and data are destroyed after relevant retention period has ended.

### Take reasonable steps to destroy,de-identify or put beyond use records and data once the retention period has elapsed.

### Seek advice where necessary from:

#### [IT], in relation to practices and procedures relating to storage and security of records, and destruction of records and data

#### [Insert name/position for person in charge of implementing this policy], in relation to determining appropriate retention periods and confirming whether certain records or data should be destroyed or retained.

## Employees, contractors and volunteers

### Consider the legal obligations relating to retention and destruction of the records and data they deal with, including obligations to:

#### retain necessary and important data

#### destroy unnecessary records and data.

## [Managers and Team Leaders] [*The particular level of manager in your organisation may need to be specified here.*]

### Ensure business units comply with their obligations under this policy.

### Assign specific roles and responsibilities to team members within business units to carry out the obligations set out in this policy.

### Provide training on records, retention periods, and destruction practices and procedures to team members.

### Undertake periodic reviews of records and data held by the business unit to ensure that records and data are being destroyed after their retention period has ended.

## Policy owner

### Communicate policy requirements to business units, managers and team leaders.

### Ensure the policy is accessible and disseminated.

### Provide organisation wide training on the requirements of the policy.

### Undertake periodic reviews of this policy and the specific retention periods set out in Appendix 1, and vary this policy as necessary from time to time.

# Additional policies

[***Link to each relevant policy if possible. Amend list based on organisation’s existing policies.***]

Privacy Policy

[##insert others as applicable]

Appendix 1: Data Retention Requirements

[***Consider whether there are specific records/data for your organisation that are not included here and need to be added. This appendix can be used generally across all business units, but can also be amended to reflect the specific records commonly used by the business units. You can also consider including the specific storage requirements of the business.***]

| Document type | Examples (non-exhaustive) | Source of obligation | Retention requirement | Destruction requirement |
| --- | --- | --- | --- | --- |
| 1. Governance and financial records | | | | |
| Written financial records that:   * correctly record and explain [##Organisation]’s transactions, financial position and performance; and * enable true and fair financial statements to be prepared and audited. | * invoices, receipts, cheques etc * documents of ‘prime entry’ (receipts and payment journals) * working papers and other documents used to explain the methods by which financial statements are made up * delivery dockets * invoices and statements issued * petty cash book * bank deposit book | *Corporations Act 2001*(Cth) ss 9, 286, 287 & 288 | Seven yearsafter the transaction covered by the records is completed. | Destroy after retention requirement. |
| Books | * Books containing the minutes or proceedings of any general meeting, or meeting of the directors | *Corporations Act 2001* (Cth) s251A | Permanently while the company operates.  For five years after the company is wound up. The liquidator must retain books for five years from date of deregistration.  For three years after deregistration former directors must keep company books. |  |
| Registers | Register of members | *Corporations Act 2001* (Cth) ss 169 & 168 | Permanently | Do not destroy. |
| Documents relevant to income and expenditure | A company carrying on a business must keep records that show and explain all transactions and other acts that are relevant for ascertaining the company’s income and expenditure. | *Income Tax Assessment Act 1936* (Cth) s 262A  *Income Tax Assessment Act 1997* (Cth) s 121–25  *Taxation Determination* TD 2007/2 | Five years after records prepared or obtained, or five years after the completion of the transactions or act to which the records related, whichever is later (subject to limited exceptions).  CGT records must be retained for five years after it becomes certain that no CGT event can happen for which those records could reasonably be expected to be relevant to working out a capital gain or loss.  A taxpayer who has incurred a tax loss should retain records relevant to ascertainment of that loss until the later of the end of the statutory record retention period or the end of the statutory period of review for the assessment of the income year when the tax loss is fully deducted or applied. | Destroy after retention requirement. |
| Payroll tax | Records to demonstrate and accurately calculate liability for payroll tax | *Payroll Tax Act 2007* (Vic) s 17C & *Taxation Administration Act 1997* (Vic) s 55  *Payroll Tax Act 2007* (NSW) *s 48 & Taxation Administration Act 1996* (NSW) s 53  *Payroll Tax Act 2009* (NT) s 74 & *Taxation Administration Act 2008* (NT) s 79  *Payroll Tax Act 1971* (Qld) s 114 & *Taxation Administration Act 2001* (Qld) s 118  *Payroll Tax Act 2008* (Tas) s 60 & *Taxation Administration Act 1997* (Tas) s 63  *Payroll Tax Act 2002* (WA) s 87 & *Taxation Administration Act* 2003 (WA) s 89 | At least five years after the payment was made or obtained, or the date of completion of the transaction or act to which it relates, whichever is later. | Destroy after retention requirement. |
| Stamp duty and duties | Records, books, documents and working papers relating to:   * transfer of property * mortgages and other security documents * leases * transfer of motor vehicles * insurance | *Duties Act 2000* (Vic) ss 21B & 21C  *Duties Act 1999* (ACT) & *Taxation Administration Act 1999* (ACT) s64  *Duties Act 1997* (NSW) & *Taxation Administration Act 1996* (NSW) s53  *Stamp Duty Act 1978* (NT) & *Taxation Administration Act 2007* (NT) s79  *Duties Act 2001* (Qld) & *Taxation Administration Act 2001* (Qld) s118  *Stamp Duties Act 1923* (SA) s48 & *Taxation Administration Act 1996* (SA) s53  *Duties Act 2001* (Tas) & *Taxation Administration Act 1997* (Tas) s63  *Duties Act 2008* (WA) &  *Taxation Administration Act* 2003 (WA) s87 | At least five years after the date payment was made or obtained, or the date of completion of the transaction or act to which it relates, whichever is later. | Destroy after retention requirement. |
| Goods and services tax | Records relevant to taxable supply, taxable importation or creditable acquisitions and importations. | *Taxation Administration Act 1953* (Cth) ss 385-5 | At least five years after the completion of the transaction or acts to which they relate. | Destroy after retention requirement. |
| Personal property security documents | Any security agreement or contract that provides for the security interest. | *Personal Property Security Act 2009* (Cth) ss 275–277 | The security agreement or contract which creates the security must be retained for the term of the security.  An interested person may ask a secured party who holds a security interest to send or make available to the interested person, or any other person, a copy of the security agreement that provides for the security interest, a statement setting out the amount or obligation that is secured pay the security interest and the terms of payment or performance.  *Note: an interested person may be:*   * *the grantor* * *a person with another security interest in the same collateral* * *an auditor of a grantor.* | Destroy after retention requirement. |
| Documents required as evidence in legal proceedings | The types of document that could be captured are broad. State and territory based legislation imposes offences in relation to the destruction of documents that a person knows are reasonably likely to be required as evidence in a legal proceeding.  For example, where there has been a workplace injury or death, the reports regarding this may be required if it is criminally investigated or if the individual initiates a civil action. | E.g. *Crimes Act 1958* (Vic) ss 83 & 254 | Necessary to determine on a case by case basis. Where litigation is on foot, or is reasonably anticipated, relevant documents must not be destroyed (even if this results in their retention for periods in excess of the time limits imposed by taxation, corporation or other legislation). | [##Organisation] must take steps as are reasonable in the circumstances not to destroy documentation that could be required as part of a legal proceeding. |
| 1. Information about individuals | | | | |
| Personal information | Any document which records information or an opinion about an identified individual or an individual who is reasonably identifiable.  For example, personal information may include:   * name, date of birth, postal address or email address of an individual * a government issued identifier (Medicare, passport or concession card number) * feedback provided in relation to an unsuccessful applicant’s job interview * professional qualifications held by an individual.   Documents such as:   * an application to attend a [##Organisation] function or conference * job applications, reference letters * those created for, or collected through, disciplinary hearings and practice audits. | *Privacy Act 1988* (Cth)  APP 11 | Retain until the personal information is no longer required for any purpose and the organisation is not legally required to retain the information. | [##Organisation] must take steps as are reasonable in the circumstances to destroy the personal information or to ensure that the personal information is de-identified when it is no longer needed and retention is not required. |
| Sensitive information, including health information | ‘Sensitive information’ is a subset of ‘personal information’ and includes information about a person’s:   * racial or ethnic origin * religious beliefs or affiliations * sexual preferences or practices * criminal record * health * political opinions * membership of a political , professional or trade association or or trade union.   Documents that might contain sensitive personal information include:   * application for attendance at a [##Organisation] function which includes religious or cultural information regarding dietary preferences * records that include the criminal history of a client, contractor or job applicant * records that include medical or health information about an individual. | *Privacy Act 1988* (Cth)  APP 11 | Retain until the sensitive information is no longer required for any purpose for which it may be used or disclosed under the Privacy Act and the organisation is not legally required to retain the information.  If the sensitive information is health information and it was collected while the person was a child, it must be retained until they reach the age of 25, or in any case seven years after the last occasion on which a health service was provided to the individual by the provider, whichever is the later.  If [##Organisation] was not the health service provider in respect of that health information, it must be destroyed or de-identified if it is no longer needed for the purpose for which it was collected or authorised under the Health Records Act. | As above, [##Organisation] must take steps that are reasonable in the circumstances to destroy the documents containing sensitive information or to ensure that the documents containing sensitive information are de-identified when they are no longer needed and retention is not required.  Where sensitive information is involved, the reasonable steps required to destroy the information under Australian Privacy Principle 11.2 by [##Organisation] may be more onerous. |
| Government related identifiers | Tax file number | *Privacy Act 1988* (Cth) ss 17 & 18  *Privacy (Tax File Number) Rule 2015 r 11* | Reasonable steps must be taken to protect the TFN information from misuse, loss, unauthorised access, modification or disclosure. Access to such documents must be restricted to individuals who need to handle the information for taxation law, personal assistance or superannuation law purposes. | A TFN recipient must take reasonable steps to securely destroy or permanently de-identify TFN information of an individual where it is no longer:   * required by law to be retained * necessary for a purpose under taxation law or superannuation law. |
| Documents that fall within the concept of personal information where the identity of the individual is reasonably identifiable, including:   * Medicare number * driver’s licence number * passport number * Centrelink number | *Privacy Act 1988* (Cth)  APP 9 & 11 | See above as for Personal Information | See above as for Personal Information. |
| 1. Employee records | | | | |
| Records of employee information prescribed by Fair Work legislation | Must keep records containing prescribed information, including:   * employee’s name, employer’s name, employee status (full-time/part-time; permanent/casual; date employment began) * records relating to pay, bonuses, allowances etc * records relating to leave * records relating to overtime * records relating to averaging of hours * records relating to superannuation contributions * records relating to termination and how employment was terminated * records relating to individual flexibility arrangements and guarantees of annual earnings. | *Fair Work Act 2009* (Cth) s 535, Ch 3, Part 3-6, Division 3  *Fair Work Regulations 2009* (Cth) | Seven years after termination of employment | Destroy after retention requirement.  ***Legal note****: Privacy Act 1988 (Cth) requirements relating to personal information and sensitive information do not apply to prescribed employee records or non-prescribed employee records (e.g. routine performance appraisals) generally*. |
| Records of transactions and other acts for the purpose of ascertaining an employer’s liability for fringe benefits tax | Documents such as:   * invoices, receipts, logbooks etc * employee declarations | *Fringe Benefits Tax Assessment Act 1986* (Cth) s 132 | Five years after the completion of the transactions or acts to which the records relate. | Destroy after retention requirement. |
| Records which record and explain all transactions and other acts engaged in by an employer, or required to be engaged in by an employer, for the purposes of superannuation guarantee | Documents such as:   * superannuation guarantee calculations; * superannuation guarantee contributions; and * choice of superannuation fund forms/nomination forms. | *Superannuation Guarantee (Administration) Act 1992* (Cth) s 79 | Five years after the records were prepared or obtained, or the transactions or acts to which those records relate, whichever is later. | Destroy after retention requirement. |
| Record of a notifiable incident involving an employee | Records of deaths, serious injuries or illness and dangerous incidents. | *Occupational Health and Safety Act 2004* (Vic) s 38  *Work Health and Safety Act 2011* (NSW) s 38  *Work Health and Safety Act 2012* (Tas) s 38  Work Health and Safety Act 2011 (ACT) s 38  *Work Health and Safety (National Uniform Legislation) Act 2011* (NT) s 38  *Work Health and Safety Act 2011* (Qld) s 38  *Work Health and Safety Act 2012* (SA) s 38 | Five years from the day notice of the incident is given to the regulator. | Destroy after retention requirement. |