Privacy Policy

Policy Name:	Privacy Policy	**Policy Number:**	2.3
Type:	Organisational	**Version:**	10
Sponsoring Manager:	EM Quality & Risk (EM Q&R)	**Revision Due:**	31/05/2027
Approved by CEO:	Louise Kelly	**Date Approved:**	30/06/2026

Contents

Introduction

Community Transitions (CT) is committed to protecting the privacy of its staff, students, volunteers, clients, residents, donors and members. CT complies with the 13 Australian Privacy Principles (APPs) under the Privacy Act 1988, which govern the collection, use, storage, and disclosure of personal information.

To support this commitment, CT has appointed a Privacy Officer responsible for ensuring compliance across all operations, including oversight through annual privacy audits and ongoing monitoring activities.

CT recognises that protecting privacy requires strong internal practices relating to the collection, handling, storage, access, retention and disposal of personal and sensitive information across all systems and service delivery functions.

Note: The Privacy & Personal Information Brochure should be offered to all CT clients when they engage with our services.

Statement of Commitment

Privacy is about protecting a person's identity - including, who they are, what they know, what they think, what they have done and what they want to do.

CT is committed to ensuring individuals maintain control over their personal information. This includes transparency about how their information is collected, used, stored and disclosed, and ensuring individuals can access and correct their information where required.

This commitment extends across all organisational practices, systems, staff responsibilities and third-party arrangements.

Scope

This policy applies to all CT, it's Board and associated entity staff, contractors, students, volunteers and third-party providers who handle personal or sensitive information on behalf of the organisation. It applies to all formats of information, including digital, paper-based, verbal and recorded information.

Privacy Principles

CT ensures compliance with the Privacy Principles through the following expanded practices:

APP	Principle	CT Practice
APP 1	Open and Transparent Management	CT maintains clearly documented processes governing the management of personal information, including this policy and associated procedures. Staff must ensure individuals are informed about: • What information is collected • Why it is collected • How it will be used and disclosed • How they can access or correct their information
APP 2	Anonymity and Pseudonymity	Where lawful and practicable, individuals may remain anonymous or use a pseudonym when interacting with CT, unless identification is required by law or is necessary to deliver services.
APP 3	Collection of Solicited Personal Information	CT will only collect information where it is: • Lawful and fair • Reasonably necessary for business activities, including service delivery, employment or compliance obligations • If an individual chooses not to give certain information, they will be advised of any potential consequences of withholding that information, which may include CT being unable to deliver the service or information requested. Information may include identifying, contact, demographic, medical, financial and other sensitive information relevant to the service provided.
APP 4	Dealing with Unsolicited Personal Information	If CT receives unsolicited personal information, it will: • Assess whether the information could have been collected under APP3 • If not, securely destroy or de-identify the information as soon as practicable, where lawful and reasonable

APP 5	**Notification of the Collection of Personal Information**	CT will take reasonable steps to notify individuals at or before collection (or as soon as practicable after) of: • The purpose of collection • Any disclosures • Access and correction rights
APP 6	**Use and Disclosure of Personal Information**	Personal information must only be used for its primary purpose, or a related secondary purpose where reasonably expected or with consent. Sensitive information will only be used or disclosed with consent or where required by law. Third-party disclosures must: • Be necessary • Include appropriate safeguards • Be governed by contractual privacy obligations Note: Subject to OPP 6.1 Child Safety & Wellbeing Policy and SA Government Information Sharing Guidelines (OPP 2.10 ISG Policy)
APP 7	**Direct Marketing**	CT does not use or disclose personal information for direct marketing purposes.
APP 8	**Cross Border Disclosure of Personal Information**	An individual's privacy is protected Australia wide by privacy laws. CT undertakes not to pass personal information to parties overseas.
APP 9	**Adoption, use or disclosure of government related identifiers**	Any data collected for reporting purposes will not identify individuals unless required and authorised by law.
APP 10	**Quality of Personal Information**	CT takes reasonable steps to ensure information is: • Accurate • Complete • Up to date This includes regular review and updating of records

APP 11	**Security of Personal Information**	CT protects personal information from misuse, loss or unauthorised access through: • Secure physical storage • Access controls and password protection • System-based security controls • Encryption and secure data handling practices All staff must immediately report suspected data breaches or security incidents. External databases (such as those provided by funding bodies) are subject to Australian Privacy Laws and comply with essential security provisions.
APP 12	**Access to Personal Information**	Individuals may request access to their personal information Requests will: • Be directed to the Privacy Officer • Be responded to within a reasonable timeframe
APP 13	**Correction of Personal Information**	The individual concerned will, (on completing the Form attached to the Privacy & Personal Information Brochure) have access to the personal information held by CT unless CT is legally unable to do so. When unable to provide access CT will advise the reason to the person concerned in writing within 30 days of the request. Individuals have the right to ask for information to be corrected or amend if the information is not accurate, complete, or up to date. The organisation must take reasonable steps to do so.

Complaints about a possible breach of privacy, where access to information has been denied, or if information has not been amended as requested, are to be directed to the Privacy Officer.

It is anticipated that issues regarding confidentially, and privacy will be dealt with by CT in the first instance. However, if more information about the legislation or assistance is required, please contact:

Office of the Australian Information Commissioner

GPO Box 5218

Sydney NSW 2001

Privacy Hotline: 1300 363 992

Website http://www.oaic.gov.au

Privacy audits

The Privacy Officer will conduct annual audits covering:

- Physical storage
- System access and password controls
- Record keeping and confidentiality practices

(See Client File Audit Form – Appendix A).

Data Retention and Disposal

Personal information will only be retained for as long as necessary, or as required by law. When no longer required, information will be securely destroyed or de-identified. CT's retention schedules and disposal procedures must be followed.

To determine the appropriate retention period, CT considers the amount, nature, and sensitivity of the personal information; the potential risk of harm from unauthorised use or disclosure; the purposes for which the information is processed and whether those purposes can be achieved through other means; and applicable legal requirements.

Collecting Personal Information

When collecting personal information, CT will ensure that it is necessary for CT's business functions and activities, such as employment, service delivery, and customer relationship management. CT collects and processes personal information only where there is a lawful basis to do so, including consent, legal obligation, or where necessary to deliver services, and where appropriate, directly from the individual.

Internal – Staff Obligations

Staff must be transparent with individuals about the collection of their information, how it will be used and disclosed, and how they can access and correct it. This transparency is communicated through privacy notices, contracts, verbal communication, and consent forms.

External – Collection from Clients and Stakeholders

The personal information CT may collect, and hold includes names, dates of birth, gender, home addresses, email addresses, telephone numbers, bank details, and information about the services and/or products provided. Information may also include identifying, contact, demographic, medical, financial and other sensitive information relevant to the service provided.

In some circumstances CT may need to collect sensitive information to provide specific services; sensitive information is only collected, held, used, and disclosed with the individual's consent or as otherwise required or permitted by law.

If an individual chooses not to provide requested personal information, they will be advised of any potential consequences, which may include CT being unable to deliver the service or information requested.

From time to time, CT may require individuals to provide personal information about other people. In such cases, CT requires that appropriate consent to release information forms be completed and that all actions are guided by relevant information-sharing guidelines.

Where appropriate, the individual providing the information must ensure that the other person has been informed that their personal information is being shared and has been made aware of this policy.

Unsolicited Personal Information

If CT receives unsolicited personal information, it will determine whether that information could have been collected under usual processes. If it is deemed it could not have been collected, CT will destroy or de-identify it as soon as practicable, provided it is lawful and reasonable to do so.

Using and Disclosing Personal Information

Internal Staff Obligations

Staff can only use personal information for the primary purpose for which it was collected, such as providing services, managing employment, or complying with legal obligations. If CT needs to use information for a related secondary purpose, it will ensure that the individual would reasonably expect this use or will obtain their consent. When disclosing personal information to third parties, staff must ensure the disclosure is necessary and that appropriate safeguards are in place. Contracts with third parties will include privacy obligations. Staff must handle sensitive information with additional care, using or disclosing it only with the individual's consent or as required by law.

Note: This provision is subject to OPP 6.1 Child Safety & Wellbeing Policy and specific to SA, the SA Government Information Sharing Guidelines as per OPP 2.10 ISG Policy.

External – Use and Disclosure

CT will only use and disclose personal information for the primary purpose of collection or as otherwise specified, which may include providing products or services, responding to enquiries, providing customer support, or complying with legal obligations. Personal information will only be used for a secondary purpose if consent has been obtained, where it is reasonably expected, or if such use or disclosure falls within a permitted exception.

Sensitive information will be used and disclosed for the primary purpose of collection, unless CT is advised otherwise, or the use or disclosure is required or permitted by law.

CT will not adopt, use, or disclose government-related identifiers unless permitted by the APPs. These identifiers will only be used or disclosed where necessary to verify an individual's identity for the provision of a service or where required or authorised by law.

Anonymity and Pseudonymity

Where practicable, CT offers individuals the option to remain anonymous or use a pseudonym when interacting with CT, unless identification is required by law or is impractical for the transaction.

Anonymity requires that an individual may deal with CT without providing any personal information or identifiers, so that CT cannot identify the individual at the time of the dealing or subsequently.

Pseudonymity requires that an individual may deal with CT using a name, term, or descriptor different from their actual name. This may include a username, an email address that does not contain the individual's actual name, or an artist's pen name or screen name.

There may be situations where anonymity or pseudonymity is not possible due to legal or operational requirements, including:

- When CT is required by law to collect an individual's identity information (e.g. for financial transactions).
- When CT provides a service that requires verification of an individual's identity (e.g. account creation).
- When responding to a specific enquiry or complaint where anonymity would hinder effective resolution.
- Where there is a legal requirement to do so (e.g. a court order).
- Where it is necessary to protect the rights and safety of others (e.g. to prevent fraud).

Ensuring Data Quality and Security

Internal – Staff obligations

CT will take reasonable steps to ensure that the personal information handled is accurate, complete, and up to date. CT will regularly review and update records to maintain data quality. CT protects personal information from misuse, interference, loss, unauthorised access, modification, or disclosure through secure physical storage, access controls and password protection, system-based security controls, and encryption and secure data handling practices. Any data breaches or security incidents must be reported immediately to a Line Manager.

External – Security of Information

CT takes reasonable steps to protect the personal information it holds from intentional and unintentional interference, loss, misuse, or unauthorised access, disclosure, or modification. CT safeguards information through written privacy policies and physical, electronic, and procedural protections.

CT holds personal information in both physical and electronic records, including through contracted cloud computing services. Computer servers used for cloud computing purposes store data in Australia. Where personal information is transferred to a contracted service provider, those providers are ordinarily contractually bound to handle personal information confidentially and securely in accordance with the APPs and the Privacy Act. External databases (such as those provided by funding bodies) are subject to Australian Privacy Laws and comply with essential security provisions.

Although care is taken to protect information provided electronically, including through CT's website, the internet is not a secure environment and the security of information during transmission cannot be guaranteed.

Access and Correction

Individuals have the right to request access to their personal information. All access requests must be directed to the Privacy Officer, who will respond within a reasonable timeframe. CT must provide access and correct any inaccuracies, incompleteness, or outdated information promptly.

Under the Privacy Act 1988 (Cth), an individual has the right to obtain access to personal information CT holds about them. There are exceptions to this right, for example, where access may impact the privacy of others or pose a threat to the individual.

Requests for access must be made in writing. Where it is reasonable to do so, CT will provide access in the manner requested.

If a request for access is refused, CT will provide written reasons for the refusal, together with details on how to make a complaint. When unable to provide access, CT will advise the reason to the person concerned in writing within 30 days of the request.

Where personal information held by CT is inaccurate, out-of-date, incomplete, irrelevant, or misleading, CT will take reasonable steps to update and/or correct it upon a written request to the Privacy Officer. There are circumstances in which CT may decline to correct information, in which case written notice will be provided.

Cross-Border Disclosure

An individual's privacy is protected Australia-wide by privacy laws. CT does not ordinarily disclose personal information to overseas recipients. Where such disclosure occurs, CT will comply with APP 8, ensuring appropriate safeguards are in place and that the disclosure is permitted by law.

Visiting Community Transitions' Website

To improve user experience, CT may use cookies. A cookie is a small text file that allows CT to collect information about a visit, including the type of browser, device, and platform used, as well as traffic patterns through the website. No personal information is stored within cookies.

If users prefer not to receive cookies, they can adjust their browser settings; however, disabling cookies may limit full website functionality. Information collected through cookies is used only for statistical and website improvement purposes. CT will not attempt to identify users or their browsing activities through cookies.

If users access another party's website via CT's website, including through links to external sites, those parties will deal with personal information in accordance with their own privacy policy. CT is not responsible for the privacy practices or the use and protection of personal information on external websites.

Marketing Communications

CT does not use personal information for marketing purposes and does not engage in direct marketing activities.

If an individual believes they have received a marketing communication from CT or has any concerns regarding the use of their personal information, they are encouraged to contact the Privacy Officer at CTEnquiries@communitytransitions.com.au.

Data Breaches and Incident Response

What is a Data Breach?

A data breach is categorised by unauthorised access, unauthorised disclosure, or loss of, any personal information held by CT, where the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

Serious Harm May Include:

- Financial fraud, including unauthorised credit card transactions or credit fraud
- Identity theft causing financial loss or emotional and psychological harm
- Family violence
- Physical harm or intimidation

Causes of a Data Breach

- Malicious action (external or internal)
- Human error
- Failures in information handling processes or security systems

Human error accounts for a significant proportion of breaches and may include:

- Accidental publication of information
- Unauthorised disclosure (written, verbal, or through insecure disposal)
- Failure to redact information
- Failure to use Blind Carbon Copy (BCC) when sending emails
- Sending information to the wrong recipient
- Loss or theft of paperwork or devices (e.g. laptops, USBs)

Regardless of the cause or scale, all data breaches have the potential to impact individuals and the organisation.

Reporting and Response

All staff must report suspected or actual data breaches to their Line Manager as soon as practicable, and within 24 hours of becoming aware of the breach.

In responding to a data breach, Community Transitions (CT) will:

- Contain the breach to prevent further exposure
- Assess the nature and scope of the breach

- Assess the risk of serious harm
- Take reasonable steps to mitigate harm
- Notify affected individuals and the OAIC where required
- Document all actions, decisions and outcomes

Significant breaches will be managed in accordance with the Notifiable Data Breaches (NDB) Scheme.

Assessment and Notification

All actual or suspected breaches must be assessed using the approved process and documentation (Appendices B and C). Where CT has reasonable grounds to believe an eligible data breach has occurred:

- The OAIC must be notified as soon as practicable
- Affected individuals must also be notified in accordance with legislative requirements

Note: The Privacy Act 1988 (section 26WH) requires that CT must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach and take all reasonable steps to ensure that the assessment is completed within 30 days after CT becomes aware.

Factors Increasing the Risk of Serious Harm

Certain types of personal information significantly increase the likelihood that an individual could suffer serious harm if involved in a data breach. The following categories elevate risk:

1. Sensitive Information

Information defined as sensitive under the Privacy Act 1988, including health or genetic information, racial or ethnic origin, political opinions or political association membership, religious or philosophical beliefs, trade union membership, sexual orientation or practices, criminal record, and certain forms of biometric information. Sensitive information is inherently higher risk because misuse could result in discrimination, humiliation, or other significant harm.

2. Identity Documents and Credentials

Documents commonly used in identity fraud, including Medicare card details, driver licence details, passport details, and Tax File Numbers (TFNs). These are particularly valuable to malicious actors and can be used to impersonate individuals or commit financial fraud.

3. Financial Information

Including bank account numbers, credit or debit card details, superannuation information, and transaction histories or credit reports. Unauthorised disclosure can directly lead to financial loss or exploitation.

4. Combined Personal Information

Risk increases when multiple data points are exposed together, even if each individual piece is low risk (e.g. full name + date of birth + address; or email + phone number + customer ID). Combined information can enable profiling, impersonation, targeted scams, or social engineering.

Training and Awareness

All staff must complete mandatory information security and privacy training upon joining CT and annually thereafter. CT conducts regular awareness campaigns through various channels, including emails, posters, and workshops. Specialised training is provided for roles with elevated data access. Compliance with training requirements is monitored and enforced.

Continuous Improvement

CT is dedicated to the continuous improvement of its information security and privacy practices. This involves regularly assessing security and privacy objectives, processes, and controls to address current risks and vulnerabilities. Feedback from incidents, audits, and staff insights are incorporated to update and enhance policies and procedures, while a structured approach to corrective actions addresses issues to prevent recurrence.

Non - Compliance

Where it is believed that a staff member has failed to comply with this policy, they will face CT's disciplinary procedure as outlined in OPP 3.6 Performance and Resolution Policy and OPP 3.13 Code of Conduct and Ethics Policy.

Definitions

Term	Definition
Anonymity	The principle that an individual can deal with an entity without being identified. The individual can protect their privacy by withholding personal details that could lead to identification
APPs	Australian Privacy Principles – the thirteen privacy principles under the Privacy Act 1988 (Cth) that regulate how organisations collect, use, disclose and manage personal information.
Commonwealth Record	Information that belongs to a Commonwealth (Federal) Government agency.
Consent	Voluntary, informed agreement by an individual to the collection, use, or disclosure of their personal information.
Cookies	Small text files placed on a user's device by a website that collect non-personal browsing information for statistical and improvement purposes.
Cross-Border Disclosure	The transfer or disclosure of personal information to a recipient located outside of Australia.
Data Breach	Unauthorised access to, disclosure of, or loss of personal information held by CT where that access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

De-identification	The process of removing identifying information from a dataset so that individual data cannot be linked to specific individuals.
Government-Related Identifier	A number or code assigned to an individual by a government agency (e.g. tax file number, Medicare number, driver's licence number).
NDB Scheme	Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth), requiring organisations to notify affected individuals and the OAIC of eligible data breaches.
OAIC	Office of the Australian Information Commissioner – the independent regulator responsible for privacy and freedom of information in Australia
Personal Information	Any information or opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not. Includes sensitive information for the purposes of this policy.
Primary Purpose	The main reason for which personal information is collected from an individual.
Privacy Act	Privacy Act 1988 (Cth) – the principal Commonwealth legislation governing the handling of personal information by Australian Government agencies and certain private sector organisations.
Privacy Officer	The designated officer at CT responsible for managing privacy compliance, conducting annual privacy audits, responding to access requests, and handling privacy complaints. This role is held by the EM Q&R.
Pseudonymity	The use of a fictitious name or identity to protect an individual's privacy
Secondary Purpose	A purpose other than the primary purpose for which personal information was collected.
Sensitive Information	A subset of personal information that includes racial or ethnic origin, political opinions, religious beliefs, sexual orientation, health information, genetic information, biometric information, criminal record, trade union membership, and political association membership. Sensitive information requires a higher standard of protection.
Solicited information	Information explicitly requested by CT under APP 3
Third Party	Any individual or organisation outside of CT that may receive or have access to personal information.
Unsolicited information	Information CT receives without request

Responsibilities

Organisation	• Maintain physical and electronic security systems protecting personal information, including secure storage, password protection, and controlled access • Ensure organisational compliance with the 13 Australian Privacy Principles (APPs) • Ensure external databases used by the organisation comply with Australian privacy laws • Ensure internal processes exist for assessment, mitigation, containment, and documentation of data breaches
Board	• Uphold CT's privacy governance framework and ensure strategic oversight of privacy compliance • Support a culture of privacy awareness across the organisation
CEO	• Review and sign off data Breach Response Form • Notifying the OAIC and affected individuals when required • Endorse and approve the Privacy Policy and oversee its organisation-wide implementation.
EMQ&R (Privacy Officer)	• Ensure an effective privacy governance framework is in place. • Conduct annual privacy audits, including physical records, digital storage, access controls, and confidentiality processes • Oversee ongoing monitoring of privacy obligations and staff compliance. • Manage all privacy-related complaints in line with the Privacy Act • Assess suspected or actual data breaches and determine eligibility under the Notifiable Data Breach (NDB) Scheme • Oversee and confirm completion of mitigation and preventative actions following any breach
Line Managers	• Receive reports of suspected or actual data breaches from staff and escalate to the Privacy Officer. • Coordinate the immediate internal response to breaches, including containment actions before executive assessment • Ensure staff comply with privacy procedures, confidentiality requirements and correct handling of personal information
Staff	• Comply with this policy in full • Complete required privacy training and handle personal information only as authorised • Follow all CT privacy procedures, confidentiality requirements, and safe-handling practices when dealing with personal information • Report any suspected or actual privacy breach immediately to their Line Manager • Only access, use, or disclose personal information when required for their role and in accordance with CT policies

	• Store and dispose of personal information securely, using approved systems and methods
Third-Party Service Providers	• Handle personal information in accordance with contractual privacy obligations consistent with the APPs and the Privacy Act 1988 (Cth) • Notify CT of any incidents or breaches affecting personal information held on CT's behalf

Supplementary Information:

Related Policy

- OPP 1.1 Continuous Quality Improvement Policy
- OPP 1.6 Document and Record Control Policy
- OPP 1.12 Acceptable use of AI policy
- OPP 2.4 Duty of Care Policy
- OPP 2.2 Confidentiality and Information Handling Policy
- OPP 2.5 Communication Policy
- OPP 2.6 Risk Management Policy and Procedure
- OPP 2.8 National Criminal History Record Screening Policy
- OPP 2.9 Subpoenas & Release of Information Policy
- OPP 2.10 Information Sharing Guidelines (ISG) Policy
- OPP 2.17 Information Security and Management Policy
- OPP 2.18 Supplier Security Policy
- OPP 3.6 Performance and Resolution Policy
- OPP 3.13 Code of Conduct and Ethics Policy
- OPP 3.21 Acceptable Use of IT Policy
- OPP 3.26 Human Resources Security Policy
- OPP 3.25 Information Security Training and Awareness Policy
- OPP 6.1 Child Safety & Wellbeing Policy
- OPP 6.2 Case Notes Files Standards & Record Audit
- OPP 6.7 Client Incidents & Reportable Death Policy

Relevant Legislation

- Fair Work Act 2009 (Cth)
- Privacy and Other Legislation Amendment Act 2024 (Cth)
- Privacy Act 1988 (Commonwealth) and Privacy Regulations 2013 (Commonwealth)
- National Disability Insurance Scheme (NDIS) Act 2013 (Commonwealth)
- Do Not Call Register Act 2006 (Cth)
- Spam Act 2003 (Cth)
- Cyber Security Act 2024 (Cth)
- Security of Critical Infrastructure Act 2018 (Cth)
- Criminal Code Act 1995 (Cth)
- Privacy and Responsible Information Sharing Act 2024 (WA)
- Children & Young People (Safety) Act 2017 (SA), Regulations 2017 (SA)
- Disability Services Act 1993 (SA), 1993 (WA)
- Guardianship & Administration Act 1993 (SA), 1990 (WA)
- Carers Recognition Act 2005 (SA), 2004 (WA)
- Children & Community Services Act 2004 (WA)
- Disability Inclusion Act 2019 (SA)
- Mental Health Act 2009 (SA), 2014 (WA)
- Aged Care Act 1997 (Commonwealth)

- Suicide Prevention Act 2021 (SA)
- Equal Opportunity Act 1984 (SA)

Supporting Documents/References

- Australian Privacy Principles (APPs) www.oaic.gov.au/privacy-law/privacy-Act/
- IT Asset End-of-Life Management Procedure
- Risk Register (Always Draft)
- Offboarding Checklist
- Supplier Register
- System Security Plan Overview
- Offboarding Checklist
- Privacy & Personal Information Brochure
- SA Information Sharing Guidelines
- WA Government Privacy and Responsible Information Sharing guidance
- Information Security Communications Plan
- Cyber Security Strategy
- Information Security Monitoring and Assurance Plan (ISMAP)
- Information Security Communications Plan
- Supplier Register
- Consent to Obtain and Release Information Form

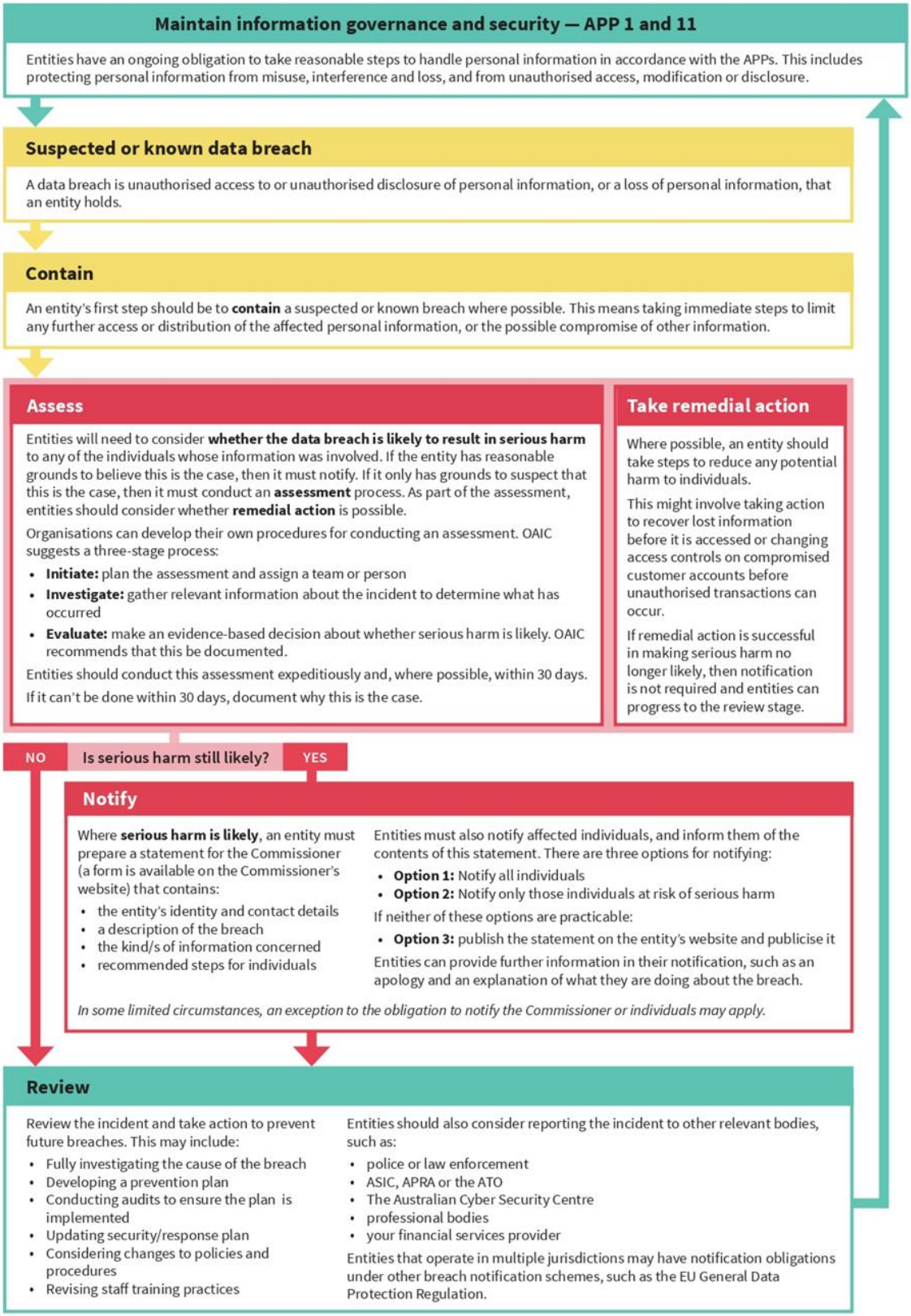
Appendices

Appendix A – Client File Audit Form

See OPP 6.2 – Appendix A – Case Note Standards and Record Audit Policy and Procedure

- Appendix B – Maintaining Information Guidelines
- Appendix C – Data Breach Response Form

Appendix B – Maintaining Information Governance



Appendix C – Data Breach Response Form

Responding to an Actual or Suspected Breach

The Privacy Act 1988 (section 26WH) requires that *the entity must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity; and take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware*

Data breaches should first be contained to prevent any further breach of personal information - prior to assessment and follow up action taking place. The aim is to limit the consequences and reduce the likelihood of affected person/s suffering harm of a data breach through responding quickly.

Data Breach Response Form	
Date: _____	
☐ Actual data breach	☐ Suspected data breach
Investigating Officer	
Assessment conducted by (name and position): _____	
Who identified/reported the data breach? How was it detected?	
Description of the data breach (what happened, what types of data/personal information is involved?)	
Number of individuals affected ☐ 1 ☐ 2 – 10 ☐ 11 – 100 ☐ 101 – 1,000	☐ 1001 – 10,000 ☐ 10,001 – 100,000 ☐ 100,001 or more OR, if known, specific number: _____
Affected Systems (Devices, email accounts, databases, worksites etc.)	
Risk Assessment (Assess and document the potential harms using the Risk Matrix).	

Mitigation and Follow- Up Actions (Include actions taken, completion dates, and responsible persons)
Notification Decision – OAIC and Affected Individuals Should the data breach be reported to OAIC through the NDB Scheme, and to affected person/s? ☐ Yes ☐ No If yes, please ensure the following information is provided to the Executive Manager for filing with the OAIC. A statement including. (a) CT Organisational name and contact details (b) a description of the data breach (c) the type of information involved (d) recommendations about the steps individuals should take in response to the data breach
Signature: Date: Once completed, please forward to the relevant Executive Manager for review, and filing within the Feedback and Complaint Register located within SharePoint Strategic Management section.
Executive Manager
On review of the information provided by the investigating officer, should the data breach be reported to OAIC through the NDB Scheme, and to affected person/s? ☐ Yes ☐ No Statements are to be submitted online at: www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach If Yes, Date Statement Lodged: _____ Copy attached? ☐ Yes ☐ No Have the affected persons been notified? ☐ Yes ☐ No If not, why not? _____ If yes, date affected persons notified: _____

Attach copies of any written communications. Store all documents within Complaints and Feedback register on SharePoint Strategic Management Tab
As soon as reasonably practical after a statement has been submitted to the OAIC, CT must: • if practical, take reasonable steps to notify the contents of the statement to each of the individuals to whom the information relates; or • if practical, take reasonable steps to notify contents of the statement to each of the individuals who are at risk from the eligible data breach. If it is not practical to undertake either of the above, a copy of the statement must be published on the CT website and reasonable steps must be taken to publicise the contents of the statement (for example, by notifying its members). The following link has suggested recommendations, dependent on the type of data breach, that should be included in the notification to person/s whose data is involved in the data breach; www.oaic.gov.au/privacy/data-breaches/respond-to-a-data-breach-notification#contactinfo
Signature: Date: Once completed, please forward to the CEO for review, and filing within the Feedback and Complaint Register located within SharePoint Strategic Management section.
CEO
Signature: Date:

Assessing the Level of Risk

Step 1 - Identify potential harms (tick all that apply):

Potential harms may include, but are not limited to:

☐ Identity theft / fraud
☐ Significant financial loss
☐ Threats to physical safety
☐ Loss of business/employment opportunities
☐ Humiliation / reputational or relationship harm
☐ Workplace or social bullying / marginalisation
☐ Other (specify): _____

Step 2 - Assess risk of serious harm

Consider:

- Whose personal information? (e.g., clients, employees, vulnerable cohorts)
- Types of information? (e.g., sensitive info, identity docs, financials, combined datasets)
- How many individuals?
- Exposure duration (how long accessible/compromised)?
- Who accessed/received it (and intent/capability to misuse)?
- Likelihood of serious harm (low / moderate / high)?
- Consequences if harm materialises (what would happen to individuals)?
- Information affected: None / Limited / Moderate / Critical
- Resulting impact on service & individuals: None / Limited / Moderate / Critical

Factors Increasing the Risk of Serious Harm

Certain types of personal information significantly increase the likelihood that an individual could suffer serious harm if the information is involved in a data breach. Serious harm may be financial, physical, psychological, reputational, or relate to identity theft.

The following categories of information elevate risk:

1. Sensitive Information

This includes information that the Privacy Act 1988 defines as “sensitive information,” such as:

- Health or genetic information
- Racial or ethnic origin
- Political opinions or political association membership
- Religious or philosophical beliefs
- Trade union membership or associations
- Sexual orientation or practices
- Criminal record
- Certain forms of biometric information

Sensitive information is inherently higher-risk because misuse could result in discrimination, humiliation, or other significant harm.

2. Identity Documents and Credentials

These are documents commonly used in identity fraud, including:

- Medicare card details
- Driver licence details
- Passport details
- Tax File Numbers (TFNs)

These items are particularly valuable to malicious actors and can be used to impersonate individuals or commit financial fraud.

3. Financial Information

This includes:

- Bank account numbers
- Credit or debit card details
- Superannuation information
- Transaction histories or credit reports

Unauthorised disclosure can directly lead to financial loss or exploitation.

4. Combined Personal Information

Risk increases when multiple data points are exposed together, even if each individual piece is low-risk. For example:

- Full name + date of birth + address
- Email + phone number + customer ID
- Employee information combined with HR or disciplinary records

Combined information can enable profiling, impersonation, targeted scams, or social engineering, increasing the likelihood of serious harm.

Using the Definitions and Risk Matrix

The above categories help assess:

- The **likelihood** that serious harm could occur
- The **severity** of potential harm if the breach is left unmitigated

These factors should be considered alongside:

- **Information affected** (None, Limited, Moderate, Critical); and
- **Resulting impact** (None, Limited, Moderate, Critical).

Information affected	Definition
None	No information was accessed, exfiltrated, changed, deleted, or otherwise compromised
Limited	Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised
Moderate	Internal, or sensitive information was accessed, exfiltrated, changed, deleted, or otherwise compromised
Critical	Protected data was accessed, exfiltrated, changed, deleted, or otherwise compromised

Resulting impact	Definition
None	No effect to the organisations ability to provide all services to all services users. No known (or likely to occur) harm caused to any person/s whose data is involved.
Limited	Some potential to interruption of services, the organisation can still provide all critical services to service users but has lost efficiency. Some inconvenience cause, but no serious harm has or is likely to occur to person/s whose data is involved.
Moderate	The organisation has lost the ability to provide critical services to a subset of the services users. Serious harm may but is unlikely to occur to person/s whose data is involved.
Critical	The organisation is no longer able to provide some critical services to any services user. Serious harm has or is likely to occur to person/s whose data is involved.

	Information affected			
Resulting impact	None	Limited	Moderate	Critical
None	Level 1	Level 1	Level 2	Level 2
Limited	Level 1	Level 2	Level 3	Level 3
Moderate	Level 2	Level 3	Level 3	Level 4

Critical	Level 2	Level 3	Level 4	Level 4

Risk Level	Action required
Level 1	File the 'Data breach response form' documenting decision making. No further action required.
Level 2	Identify appropriate mitigation, remedial and future prevention actions and carry out identified actions. File the 'Data breach response form' documenting decision making.
Level 3	A notification to the NDB Scheme may be required unless immediate mitigation action can further reduce the likelihood of serious harm. If likelihood of serious harm cannot be mitigated, actions from 'Level 5' should be undertaken. Identify appropriate mitigation, remedial and future prevention actions and carry out identified actions. File the 'Data breach response form' documenting decision making.
Level 4	Notification to the NDB Scheme required. Person/s whose data is involved in the data breach must be notified. Immediately escalate to CEO for formal response, including public response, where required. Identify appropriate mitigation, remedial and future prevention actions and carry out identified actions. File the 'Data breach response form' documenting decision making.

Step 4 – Apply any required actions for the level selected

Once the risk level has been determined, the corresponding actions must be implemented without delay. All decisions, actions taken, and rationale must be clearly documented in the Data Breach Response Form to ensure accountability and compliance with regulatory requirements.