Policy	Data Retention
Audience	This policy applies to all Team Members and the Board

1. Policy Statements

Canteen is committed to managing data in a lawful, secure and risk-based manner that protects the privacy of individuals and supports good governance, and will:

- Collect, retain, de-identify and dispose of data in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and other applicable legislation.
- Retain data only for as long as it is required to meet legal, regulatory, operational and business needs.
- Securely destroy or de-identify personal and sensitive information when it is no longer required or permitted to be retained.
- Apply consistent retention and disposal rules across systems, based on data category, risk and system of record.
- Ensure access to data is restricted to authorised personnel and is proportionate to business need.
- Preserve data where required for litigation, regulatory inquiries, audits or investigations.

2. Purpose

The purpose of the Data Retention Policy and Schedule is to :

- define Canteen's approach to retaining, protecting, de-identifying and disposing of data in a lawful, consistent and risk-based manner
- establish clear retention periods by data category and system
- reduce privacy, cyber and compliance risk
- support consistent, auditable and lawful data management and governance practices

3. Policy

3.1. Retention Periods

Data is required to be retained in accordance with the following requirements:

3.1.1. Formal or Official Records

Any Data that is part of any categories listed in the Data Retention Schedule contained in Schedule 1 to this Policy, must be retained for at least the amount of time indicated in the Data Retention Schedule.

3.1.2. Disposable Information

- The Data Retention Schedule will not set out a retention period
- Data should only be retained as long as it is needed for business purposes and then securely disposed of
- If Data is not listed in the Data Retention Schedule, it must be assessed before disposal to ensure no other legal, regulatory, or business requirements apply.

3.1.3. Personal Information

The Privacy Act requires Canteen to take reasonable steps to Protect Personal Information (PI, including Sensitive Information) and to destroy or de-identify PI once it is no longer needed for any purpose for which it may be used or disclosed under the APPS (subject to legal requirements for retention of the data, other laws and where PI is contained in a Commonwealth record).

3.1.3.1. PI Data Retention Business Rules

- Canteen holds PI across multiple systems
- PI data is further classified by the following data categories:
  - Client
  - Supporter
  - Employee
  - Supplier
  - Financial
- The PI data category, in conjunction with the system in which data is in, work together to define (system specific) data retention rules that:
  - meet legislative requirements
  - meet business processing needs
  - minimises the amount and duplication of PI data across Canteen systems
  - minimises the material impact if Canteen data was breached

System	Client	Supporter	Employee	Supplier	Financial
Salesforce	✓	✓			

Client Data

- Adult Client Data: deleted after 7 years of client inactivity, i.e duration of the individual's involvement with Canteen plus seven years.
- Child Health Information Data: retain until the individual turns 25
- Client Data is not deleted where the associated account has a Child Safety / Open Disclosure / Stolen Generation / Guardianship of the Government Indicator

Supporter Data

- De-identified after 7 years of inactivity, i.e the last donation was processed 7 years ago

Note: Donor PI data from the following sources are entered into Salesforce. The same business rules referenced above apply, noting the 'original source' data is destroyed post entry into Salesforce. Refer to Section 3.2.2 for more detail.

Original Source Document

- Sign Up Forms
- Paper based Donation Forms
- External Agency Campaign Files

System	Client	Supporter	Employee	Supplier	Financial
Employment Hero			✓		✓

Employee Data

- deleted 7 years after the employee has left Canteen unless there is an active workers compensation claim and / or legal proceedings

Job Applicant Data

- deleted after 12 months

System	Client	Supporter	Employee	Supplier	Financial
NetSuite		✓	✓	✓	

Supporter Data

- consists of Contact Name and Contact ID with no data retention period specified

Employee Data

- deleted 7 years after the employee has left Canteen

Supplier Data

- Supplier's account profile deleted 7 years after the last processed transaction

System	Client	Supporter	Employee	Supplier	Financial
FlexiPurchase			✓		

Employee Data

- deleted 7 years after the employee has left Canteen

System	Client	Supporter	Employee	Supplier	Financial
Digital Canteen Connect	✓				✓

- When the SalesForce Canteen Connect Last Login field contains a date that is more than 7 years old -the Client Data in Canteen Connect is de-identified
- Web chats / Posts are retained to present the integrity of existing conversations
- Canteen Connect users under a court order – associated data is retained

System	Client	Supporter	Employee	Supplier	Financial
Digital - Corporate - The Shop - Donation Page	✓	✓			

- data is deleted after 6 months post ingestion of PI data into SalesForce
- Reports that are accessed for historical information are retained for 6 months

System	Client	Supporter	Employee	Supplier	Financial
Microsoft 365	✓	✓	✓	✓	✓

- Deleted after 7 years based on:
  - Creation / edit date
  - Category label
  - Legislative requirements

3.1.3.2. 'Other' Data Retention Business Rules

- Please refer to Schedule 1 for a tabulated overview of the data retention business rules for other types of 'data' and information held by Canteen

3.2. Storage, Back Up and Disposal of Data

3.2.1. Storage

- Canteen's data must be stored in a safe, secure and accessible manner
- Any document and financial files that are essential to our business must be duplicated or backed up at least once per week and maintained offsite or both

3.2.2. Destruction

- Data and Tech Team is responsible for the continuing process of identifying the Data that has met required retention period and supervising its destruction or de-identification
- Non confidential Data may be destroyed by recycling

3.2.3. De-identification

- The Data and Tech team may determine that PI should be deidentified as opposed to destroyed and will oversee the de-identification process

3.3. Preservation of Documents for Contemplation, Litigation and Other Special Circumstances

- All data destruction must cease immediately upon notification that records are required to be preserved for actual or reasonably anticipated litigation (a litigation hold).
- Routine destruction activities may only resume once the litigation hold is formally lifted by the relevant Executive Team member (or delegated authority).
- Notwithstanding any approved Data Retention Schedule, all Team Members and Volunteers, must preserve records where they are aware, or have been notified, that records may be relevant to:
    - current or anticipated litigation
    - regulatory or government investigations
    - audits or reviews
    - any other matter requiring preservation
- This includes a strict prohibition on deleting, altering, or disposing of affected records, including emails and electronic data.
- Preservation requires:
    - suspension of applicable retention and destruction timeframes
    - maintaining records in their original format where possible
    - protecting the integrity and completeness of records
- Records must be retained until it has been formally advised retention is no longer required.

- Routine data disposal processes may also be suspended in other circumstances, eg: mergers, acquisitions, system migrations, or major technology changes.

3.4. Compliance

- Non-compliance may subject Canteen to serious civil and / or criminal liability
- Compliance with this Policy may be monitored via periodic checks and audits
- All Team Members and Volunteers must promptly report any suspected or actual non-compliance with the Policy (including unauthorised destruction, alteration, concealment or retention of data) in accordance with Canteen's incident reporting and escalation processes. Refer to the *Incident Management Policy* and Procedure and the *Whistle Blower Policy*
- Certain actual or potential breaches of this Policy will require Canteen to make formal notification to government regulators. Refer to the *Data Breach Response Guideline.*

4. Responsibilities

4.1. All Canteen team members

All Canteen team members are responsible for:

- Complying with this Policy and the Data Retention Schedule
- Advise the Risk and Compliance Lead of any data held that is not referenced in the Data Retention Policy and Schedule

4.2. Risk and Compliance Lead

In addition to 4.1 the Risk and Compliance Lead is responsible for monitoring the internal and external environment in relation to data protection and data retention laws which regulate data, including PI

4.3. Data and Tech

In addition to 4.1, the Data and Tech team is responsible for the continuing process of identifying the Data that has meets required retention period and supervising its destruction or de-identification

4.4. Executive

In addition to 4.1, the Executive Team is responsible for:

- Approving and overseeing the Data Retention Policy and ensuring alignment with legal, regulatory, and organisational requirements
- Authorising exceptions, including litigation holds, disposal suspensions, and deviations from the Data Retention Schedule

5. Definitions

- Confidential Information Any non-public information that is disclosed, accessed, or created in the course of Canteen's activities, which is intended to be kept confidential or is reasonably expected to be confidential, and which may cause harm to individuals or the organisation if disclosed without authorisation.
- Data - Any information created, collected, stored, or processed by Canteen, in any format, including electronic and physical records.
- Data Retention - The practice of storing Data for a defined period to meet legal, regulatory, operational, and business requirements.
- Data Retention Schedule - The approved framework that specifies minimum retention periods and disposal requirements for different categories of data.
- De-identification - The process of removing or altering personal identifiers so that an individual is no longer reasonably identifiable.
- Disposal / Destruction - The authorised process of permanently deleting or securely destroying Data so that it cannot be reconstructed or recovered.
- Formal or Official Record - Data identified as requiring retention due to legal obligations, evidentiary value, or its importance to business operations, eg: Board Minutes
- Health Records: Any information relating to a Canteen service user's physical or mental health, or the provision of a health or psychosocial support service by Canteen, including assessments, case notes, care plans, medical history, and service interactions.
- Litigation Hold (Legal Hold) - A directive requiring the immediate suspension of routine data destruction to preserve Records relevant to actual or reasonably anticipated litigation, investigation, or audit.
- Personal Information - Information or an opinion about an identified individual, or an individual who is reasonably identifiable, as defined under the Privacy Act 1988 (Cth).
- Record - Data that is retained as evidence of business activities, decisions, or transactions, and that must be managed in accordance with retention requirements.
- Sensitive Information - A subset of Personal Information that is afforded a higher level of protection under the Privacy Act 1988 (Cth) (e.g. health information, racial or ethnic origin, or criminal history).

6. Related documents

Legislation Standards Contracts	• Privacy Act 1988 (Cth) • Australian Privacy Principles • Corporation Act 2001 • Australian Charities and Not-for-profits Commission Act 2012 • Charitable Fundraising Act 1991 (NSW); • Charitable Collections Act 2003 (ACT). • Fundraising Act 1998 (Vic). • Fair Work Act 2009 (Cth) • Fair Work Regulations 2009 (Cth) • Privacy (Tax File Number) Rule 2015 (Cth) • Health Records Act 2002 (NSW) s 25(1).
National Safety and Quality Digital Mental Health Standards	• Action 1.31 -Transparency
National Principles for Child Safe Organisations	• Principle 1 – Governance and Leadership
Internal policies, procedures and supporting documents	• Privacy Policy • Personal Information Consent Form • Whistleblower Policy • Charter of Service User Rights • Service User Records Policy & Procedure • Information and Data Security Policy • Data breach Guideline • Digital Platforms Data Security • Digital Disaster Recovery Procedure • Incident Management Policy and Procedure • Internet and Business Communication Tools Policy

7. Governance

Canteen Policy:
Location: Policy Library > Operations > Risk and Compliance

Effective date	May 2026	Review date	May 2029
Policy owner: Raul Caceres		Endorsement Level: Executive	
Endorsement Signature		Printed Name	Raul Caceres

Schedule 1 – Canteen Data Retention Schedule

A reference to a limitation period in the tables below refers to the limitation periods contained in the relevant state and territory limitations acts (for example in NSW the Limitation Act 1969 (NSW)). This legislation sets out the deadline for filing a claim in certain matters (e.g. breach of contract or personal injury), it is important for Canteen to retain this information for the length of the relevant limitation period in the event a legal claim is brought.

Company and Corporate Records	Retention Period	Comments
Accounting records	Seven years after transactions are completed	Corporations Act 2001 (Cth) ss 286–289, 1306; best practice. Other legislation (e.g. tax) may require longer. Electronic records must be convertible to hard copy and accessible within a reasonable time.
Register of members, debenture holders or option holders	Indefinitely (former member entries may be removed after 7 years)	Corporations Act 2001 (Cth) ss 173(1), 169(7); best practice. Registers must be available for inspection by any person.
Historical records and archives	Indefinitely	Usual practice; no prescribed legal period. Retained for historical and organisational purposes.
ACNC reporting information (financial and operational records)	Seven years after transactions, operations or acts are complete	Australian Charities and Not-for-profits Commission Act 2012 (Cth) s 55-5. Applies to fundraising where state/territory requirements are not otherwise specified.

Fundraising Records	Retention Period	Comments
NSW fundraising information (participants, cash books, asset register, receipts, minutes)	Accounting records: 7 years; Other records: 3 years	Charitable Fundraising Act 1991 (NSW); NSW Charitable Fundraising Guidelines. Note: Canteen will retail these records for 7 years to ensure alignment with broader financial, taxation and governance obligations, including the ATO and ACNC requirements.

Fundraising Records	Retention Period	Comments
ACT fundraising information (income/expenditure records, audit-ready records)	7 years	Charitable Collections Act 2003 (ACT). If collection spans multiple jurisdictions, total collection amount may be recorded rather than ACT-specific portion.
VIC fundraising information (financial, primary accounts, summary accounts)	3 years after the Fundraising Appeal ends	Fundraising Act 1998 (Vic). Summary accounts not required to be Victoria-specific for national fundraising activities. Note: Canteen will retain these records for 7 years to ensure alignment with broader financial, taxation and governance obligations, including the ATO and ACNC requirements.
Communications with State/Territory fundraising regulators	7 years	Based on limitation periods. Includes notices of activities and regulator correspondence; required for demonstrating compliance obligations.

Team Member and Volunteer Records	Retention Period	Comments
Employee records (employment details, contracts, pay, leave, termination)	At least 7 years after termination of employment	Fair Work Act 2009 (Cth) s 535; Fair Work Regulations 2009 (Cth) regs 3.31–3.40.
Superannuation contribution records	At least 7 years after termination of employment	Fair Work Act 2009 (Cth) s 535; Fair Work Regulations 2009 (Cth) reg 3.37. Additional requirements may apply under the Superannuation Industry (Supervision) Act 1994 (Cth).
Tax file number (TFN) information	Retain only as long as required; securely destroy or de-identify when no longer required	Privacy (Tax File Number) Rule 2015 (Cth) s 11(2). Requires secure destruction or de-identification when no longer needed for lawful purposes.

Team Member and Volunteer Records	Retention Period	Comments
Volunteer records (contact details, checks, training, participation)	7 years from end of volunteer engagement	Based on limitation periods; includes certifications such as Working With Children Checks and training records.

Client and Sensitive Data	Retention Period	Comments
Personal Information of service users (contact details, demographics, interactions, non-sensitive data)	Duration of involvement plus 7 years	Based on limitation periods and Privacy Act 1988 (Cth) APP 11.
Sensitive information of service users (health, cultural background, relationships, personal circumstances)	Duration of involvement plus 7 years (or shorter where appropriate)	Limitation periods and APP 11. Should only be retained as long as reasonably necessary. Consider earlier destruction due to sensitivity and risk.
Health information (health services provided)	Adults: 7 years from last service Minors: until age 25; Destruction logs: indefinitely	Health Records Act 2002 (NSW) s 25(1). Must retain minimum statutory periods and maintain records of destruction.
Records relating to Indigenous individuals or children removed from families	Indefinitely (with informed consent)	Recommendation from Bringing Them Home Report (1997).
Child sexual abuse records (allegations, actions, support records)	45 years	Royal Commission into Institutional Responses to Child Sexual Abuse (Recommendation 8.1).

Facilities and IT Records	Retention Period	Comments
CCTV recordings	30 days (routine); longer where required for investigations or claims	Business need; Privacy Act 1988 (Cth) APP 11; limitation periods; AS 4806–2006. Retain only as long as necessary. Additional notice requirements apply in NSW/ACT; more complex rules for audio recordings.
Visitor logs	7 years	Based on limitation periods and Privacy Act 1988 (Cth) APP 11.
Internal IT systems documentation	5 years from decommissioning	Business need; no prescribed statutory period.
System monitoring logs (security, performance, threat detection)	7 years	No strict statutory requirement; aligns with government guidance. Supports incident investigation, cyber risk management, and dispute resolution.
Business continuity and information security plans	7 years from when superseded	Business need; may be required by contracts or legal obligations. Retain for audit, assurance, and potential disputes.
System backups	6 months (default), unless otherwise specified	Business need; retention may vary depending on system, risk, or policy exceptions.

Marketing	Retention Period	Comments
Purchased mailing lists and associated contracts	Mailing lists: 1 year; Contracts: 7 years from expiry/termination (12 years if executed as a deed)	Best practice for mailing lists; limitation periods for contracts. Personal information must only be retained as long as reasonably necessary (Privacy Act APP 11).
Customer and donor relationship records (interactions, queries, feedback, account history)	7 years from last contact	Business need and limitation periods.

Marketing	Retention Period	Comments
Marketing opt-out / suppression lists	Indefinitely	Business need; Spam Act 2003 (Cth); Do Not Call Register Act 2006 (Cth); Privacy Act APP 7. Retain only information necessary to honour opt-out requests.
Marketing consent records	While consent is valid; then 7 years from withdrawal or expiry	Business need; limitation periods; Spam Act 2003 (Cth); Do Not Call Register Act 2006 (Cth); Privacy Act APP 7. Consent may be withdrawn at any time.
Press releases	5 years from publication	Business need; no specific statutory requirement.
Customer complaints records	7 years from closure	Business need and limitation periods.
Website analytics data (cookies, tracking technologies)	2 years	Business need. Cookie durations may vary depending on function.

Legal Records	Retention Period	Comments
Contractual documents	Contract term plus 6 years (12 years if executed as a deed)	Based on limitation periods for contractual claims.
Superseded policy documents	6 years from being superseded	Based on limitation periods and business need for audit and governance purposes.
Insurance claims records	6 years after settlement	Based on limitation periods for potential claims or disputes.
Work health and safety notifiable incident records	5 years from date of notification	Work Health and Safety Act 2011 (Cth) s 38(7) and equivalent state legislation.
Intellectual property records (trademarks, patents, moral rights waivers)	6 years from expiry of the relevant right	Based on limitation periods.