DATA RETENTION AND DESTRUCTION

Policy: Data Retention Policy	**Version: Two**
Drafted By: P Pynor	**Approved by Board on May 12, 2025**
Responsible Person: Board Chair	**Scheduled Review Date: May 12, 2027**

Introduction

This Policy sets out One Foundation's approach to managing, retaining and destroying records and data (including personal information) we hold.

This Policy aims to outline roles, responsibilities and steps One Foundation will take when dealing with record and data retention and destruction.

Effective as of April 1, 2024, this Data Policy outlines the protocols and guidelines governing the collection, usage, and protection of data within our organization. It is important to note that the provisions detailed herein apply solely from this day forward. This policy marks a commitment to responsible data management practices, ensuring the privacy, security, and ethical treatment of all data under our stewardship.

Scope

This policy should be read in conjunction with One Foundation's Cyber Security Policy, which outlines measures to safeguard data confidentiality, system access, and breach response protocols. Together, these policies support responsible data stewardship and legal compliance.

What do we mean by 'record' and 'data'?

The Privacy Act provides that a 'record' can be a paper or electronic file. Records may include physical documents, digital scans of documents, databases, and electronic files such as text, image, video, or audio files. Any medium that captures and contains information constitutes a 'record'.

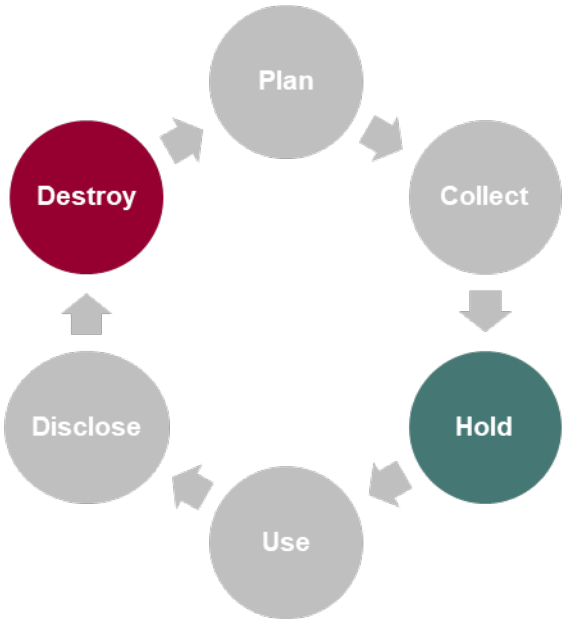
In this Policy, 'data' means any information contained in a record, including (but not limited to) personal information.

Who does this Policy apply to?

This Policy applies to all Board Members and employees, including temporary employees, contractors, and volunteers who have access to One Foundation records and data or are involved in collecting, storing or securing records and data on behalf of the Foundation.

General rules and principles

Information lifecycle



- The information lifecycle describes each phase of One Foundation's 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 de-identifying that information so that it is no longer considered personal information.
- The Privacy Act requires us to delete personal information when no longer needed (including any legal purpose). Still, data retention laws may require us to keep that personal information for specific periods. 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 below when managing, retaining and destroying records and data.

Secure Digital Data Destruction

When digital records are no longer required:

- Use secure deletion tools that permanently erase files and prevent recovery.
- Physically destroy storage devices if needed (e.g., degaussing, shredding hard drives).
- Ensure destruction methods are appropriate to the classification level (e.g., Red-level
- data must not be left on standard recycling paths).

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 necessary for 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.
- 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 required for business functions or to comply with legal obligations.
- Consider whether there are any contractual obligations to destroy certain records and data after the expiration of a contractual relationship.

- Record data in the most appropriate format and minimize paper records. Scan physical documents and save the digital scans in One Foundation International G Drive. Do not use your email inbox as a record filing system.
- Take steps to secure your records and data and minimize the risk of data corruption or accidental loss. Ensure that essential data is securely backed up and archive records when they are not actively being used (but are not ready to be destroyed).
- Ensure data can be easily located and accessed (even when archived or inactive).
- Ensure paper records are securely destroyed if appropriate. Use shredders or security bins to destroy paper records.

Data Classification for Retention Purposes

One Foundation uses a data classification system to guide security and retention standards:

- Red: Confidential and sensitive data (e.g., financial details, personal identifiers).
- Green: Internal use data (e.g., project notes, non-sensitive operations).
- White: Non-sensitive development/test data.
- Black: Publicly accessible data (e.g., website content).

Retention of Red data must follow the highest level of control and shortest practical retention period. Destruction must be secure and irreversible.

Roles and responsibilities.

Employees, contractors and volunteers

- Consider the legal obligations relating to retention and destruction of the records and data they deal with, including obligations to:
  (a) retain necessary and important data
  (b) destroy unnecessary records and data.

Managers

- 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.

Board

- Communicate policy requirements to business units, managers and team leaders.
- Ensure the Policy is accessible and disseminated.
- Provide organization-wide training on the requirements of the Policy.
- Undertake periodic reviews of this Policy and the specific retention periods set out in Data Retention Profile and vary this Policy as necessary from time to time.

Incident Response and Data Breaches

In the event of a data breach or security incident affecting retained data:

- Staff must immediately follow the breach response steps outlined in the Cyber Security
- Policy Addendum.
- Any breach involving Red-classified data must be assessed within 30 days and may

- require notification to affected parties and the OAIC.
- The Data Breach Response Form must be completed and retained for future review.

AUTHORISATION

Michael Chant
Interim OFI Board Chair

Appendix: Data Retention Profile

Data Type	Classification	Retention Period	Disposal Method
Employee records	Red	7 years post-employment	Secure digital erase / shred
Donor information	Red	7 years post-donation	Secure digital erase
Financial records (e.g. invoices)	Green	7 years	Archive then delete / shred
General communications	Green	2 years	Delete digitally
Project photos (with consent)	Green	Until withdrawn or 5 yrs	Delete securely
Web content / public reports	Black	As needed	Public access; no secure disposal