

March 2025

INTERNAL

Data Retention and Disposal Policy

FUNDS  AXIS

Policy title:	Data Retention and Disposal Policy
----------------------	------------------------------------

Issue	1.2
Approved by:	Darren Burrows
Approval Date:	September 2024
Next Review Date:	September 2025

Scope:	The policy applies to all data held, how long we hold for and ow it is disposed according to legally compliant standards of data protection and data security.
Associated documentation:	<ul style="list-style-type: none"> \ Employee Privacy Notice \ Job Applicant Privacy Notice \ Privacy & Cookies Policy \ Data Sharing Agreement – 3rd Party \ GDPR Impact Assessment
Responsibility for Implementation & Training:	Day to day responsibility for implementation: ISO

Distribution methods:	Methods used to communicate this policy: <ul style="list-style-type: none"> • Information Security Training Module
------------------------------	---

Data Retention and Disposal Policy

Introduction

While carrying out various functions, we create and hold a wide range of recorded information. Records will be properly retained to enable us to meet our business needs, legal requirements, to evidence events or agreements in the event of allegations or disputes and to ensure that any records of historic value are preserved.

- the untimely destruction of records could affect:
- the conduct of the business;
- the ability of the business to defend or instigate legal actions;
- the business's ability to comply with statutory obligations, and/or
- the business's reputation.

Conversely, the permanent retention of records is undesirable and, in certain circumstances, unlawful. Therefore, disposal is necessary to free up storage space, reduce administrative burden, and to ensure that the organisation does not unlawfully retain records for longer than necessary, particularly those containing personal data.

This policy supports our organisation in demonstrating accountability through the proper retention of records and by demonstrating that disposal decisions are taken with proper authority and in accordance with due process

Purpose

The purpose of this policy is to provide guidance as to set out the length of time that records should be retained and the process to review the records as to any further retention or for disposing of records at the end of the retention period. The policy helps to ensure that we operate in compliance with the General Data Protection Regulation and any other legislative or regulatory retention obligations.

Scope

The policy covers the records listed in the Data Processed Register, irrespective of the media on which they are created or held, including:

- paper;
- electronic files (including database, Word documents, power point presentations, spreadsheets, web pages and e-mails); and
- photographs, scanned images, CD-ROMs, and videotapes.

The policy covers all types of records that we create or hold which may include but are not limited to:

- employee data;
- customer data;
- minutes of meetings;
- data from external parties;
- contracts and invoices;
- registers;
- legal advice;
- file notes;
- financial accounts; and
- the organisation's publications.

Application

The policy applies equally to all permanent and casual employees, agency staff, and outsourced suppliers.

Minimum Retention Period

Unless a record has been marked for 'permanent preservation' it should only be retained for a limited period of time. A recommended minimum retention period is provided for each category of record in the Data Processed Register. The retention period applies to all records within that category.

The recommended minimum retention period derives from either:

- business need;
- legislation;
- responding to complaints;
- taking or defending legal action

The current agreed data retention periods are set out in Appendix 1.

Disposal

The Data Protection Officer is responsible for ensuring that data is periodically reviewed (at least annually) to determine whether any retention periods have expired. Once the retention period has expired, the data must be reviewed, and a disposal action agreed upon.

A disposal action is:

- the destruction of the data; or
- the retention of the data for a further period; or,
- alternative disposal of the data.

The disposal action decision must be reached having regard to:

- on-going business and accountability needs (including audit);
- current applicable legislation;
- whether the data has any long-term historical or research value;
- best practice in the business industry;
- costs associated with continued storage versus costs of destruction; and
- the legal, political, and reputational risks associated with keeping, destroying, or losing control over the data.

Decisions must not be made with the intent of denying access or destroying evidence.

Destruction

No destruction of data should take place without assurance that:

- the data is no longer required by any part of the business;
- no work is outstanding by any part of the business;
- no litigation or investigation is current or pending which affects the data; and
- there are no current or pending Freedom of Information or Data Protection access requests which affect the data.

[All disposals must be recorded on the Data Disposal Record, see Appendix 2.]

Destruction of Paper Records

Destruction should be carried out in a way that preserves the confidentiality of the data. Non-confidential data can be placed in ordinary rubbish bins or recycling bins. Confidential data should be placed in confidential waste bins or shredded and placed in paper rubbish sacks for collection by an approved disposal firm. All copies, including security copies, preservation copies and backup copies, should be destroyed at the same time and in the same manner.

Destruction of Electronic Records

All electronic data will need to be either physically destroyed or wiped in keeping with the organisation's Security Policy. Deletion of the files is not sufficient.

Further Retention

The data may be retained for a further period if it has on-going business value or if there is specific legislation that requires it to be held for a further period. Data should not ordinarily be retained for more than 30 years in aggregate from the date of creation, save for human resources information that may need to be retained for 100 years from date of birth.

Further Information

This document should be read in conjunction with the Data Protection Policy and Data Security Policy.

DATA RETENTION TABLE

Employee & Contractors Records Retention Periods			
RECORD	RETENTION PERIOD	OWNER	CLASSIFICATION
EMPLOYEE & CONTRACTOR DATA	(From last effective date or termination of employment/contractor as appropriate)		
Contact details	1 year	HR Dept	Confidential
Date of birth	6 years	HR Dept	Confidential
Gender	6 years	HR Dept	Confidential
Marital Status	1 year	HR Dept	Confidential
Beneficiary and emergency contact information	1 year	HR Dept	Confidential
Government identification numbers	6 years	HR Dept	Confidential
Education and training details	1 year	HR Dept	Confidential
Benefits descriptions per employee	3 years	HR Dept	Confidential
Collective bargaining agreements	3 years	HR Dept	Confidential
Employee applications and CVs	1 year	HR Dept	Confidential
Recruitment documents	1 year	HR Dept	Confidential
Background checks on employees	5 years	HR Dept	Confidential
Employment contracts	3 years from their last effective date	HR Dept	Confidential
Payroll records	6 years	HR Dept	Confidential
Tax information	6 years	HR Dept	Confidential
Injury and Illness Incident Reports	As long as relevant plus 1 year	HR Dept	Confidential
Job descriptions	2 years	HR Dept	Confidential
Performance plans and records	2 years	HR Dept	Confidential
Disciplinary records	2 years	HR Dept	Confidential
Sickness records	2 years (following end of current year)	HR Dept	Confidential
Holiday records	2 years	HR Dept	Confidential
Pension plan information	Duration of employment plus 1 year	HR Dept	Confidential
Equality monitoring	6 years	HR Dept	Confidential
Insurance claims/ applications	3 years after completion	HR Dept	Confidential
Insurance contracts and policies	6 years after expiration	HR Dept	Confidential
Photographs	1 year	HR Dept	Confidential

Recruitment and Job Applicant Records Retention Periods			
RECORD	RETENTION PERIOD	OWNER	CLASSIFICATION
RECRUITMENT	(From last effective date after the end of the relevant recruitment process)		
CV details (if unsuccessful)	6 months	HR Dept	Confidential
CV Details (future consideration)	1 year	HR Dept	Confidential
CV Details (successful)	Refer to employee table	HR Dept	Confidential

<u>Marketing Records Retention Periods</u>			
RECORD	RETENTION PERIOD	OWNER	CLASSIFICATION
MARKETING	(From last effective date after the end of the relevant enquiry or mailing list process)		
Name, company name, company address, contact details	6 months (from enquiry with no progress)	Marketing Dept	Internal
Name, company name, company address, contact details	Can unsubscribe from mailing list at anytime	Marketing Dept	Internal
Name, company name, company address, contact details	Refer to Customer table	Marketing Dept	Internal

<u>Customer Records Retention Periods</u>			
RECORD	RETENTION PERIOD	OWNER	CLASSIFICATION
CUSTOMER	(From last effective date after the end of the relevant customer cancellation period)		
Name, company name, company address, contact details, job title	2 years	All Depts	Internal
Accounts Dept contact details & BACS transfer details	2 years	Finance Dept	Restricted
Data to include investment funds but excluding client data	2 years	All Depts	Internal

Any emails containing personal data falling under the above categories will be kept with your personnel information and disposed of in accordance with the above schedule. We reserve the right to amend this table from time to time, as necessary.

Appendix 2

<u>Data Disposal Record</u>					
Data Type	Start date of data	Date due to be disposed	Actual disposal date	Disposal Method	Rationale