Document Retention Policy & Procedure

INTRODUCTION

Data Protection legislation (Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)) contains requirements impacting records retention, namely that personal data should not be retained for excessive periods and must be stored and disposed of securely. The retention periods for many financial/legal documents must comply with mandatory requirements of external organisations such as HM Revenue and Customs and funding providers.

Health and Safety legislation requires the retention of key health and safety reports and documentation, and Employment legislation requires the retention of records on current and past employees. The management, retention, and disposal of documents can be a costly operation, and it is important that only records defined in this document are retained. All appointed subcontractors are required to meet their legal and funding requirements and adhere to this policy.

Records must also be retained in accordance with any contractual requirements set out in funding agreements, service contracts, or other legal agreements entered into by Step Ahead. Where contractual retention periods exceed statutory requirements, the longer retention period will apply.

PURPOSE AND SCOPE

This document aims to provide clear directives for the retention, storage, and disposal of key documents generated and received by Step Ahead. Specifically:

- To ensure that records required to be kept for legal/statutory reasons are retained for the appropriate period and in a manner that allows them to be retrieved and admissible as evidence.
- To ensure the efficient, controlled, and appropriate disposal of records that are no longer needed.

The term 'document' includes records in all media and formats and includes electronic records.

The following categories of records are not specifically included in the policy because their value depends entirely on their context and content:

- General correspondence
- Reports
- Meeting documents (agenda, minutes, etc.)

Retention and disposal schedules and procedures should, at a minimum:

- Identify which documents and records should be retained and the minimum retention periods for each record type.
- Identify procedures for selecting records for retention or disposal and the frequency with which that selection process should take place.

POLICY

Records Retention Schedule

Step Ahead's retention schedule is regularly reviewed to ensure compliance with any changes. The schedule includes details about the document owner and the legislative context (where applicable) for retention of the document(s). Any records not included in the retention schedule should be maintained for a minimum of 3 years. If staff are in any doubt as to whether documents should be retained or destroyed, they should refer the matter to Corporate Support.

Legal Hold

Where records are subject to litigation, audit, investigation, Freedom of Information request, safeguarding concern, or any formal legal or regulatory inquiry, a legal hold will be applied. Records under legal hold must not be altered, deleted, or destroyed until formal authorisation for release is given by Corporate Support or the relevant authorised lead.

Procedure

1. Archiving of electronic records

1.1 Participant records are limited to documents relating to:

- Participant Data
- Funded Educational Support
- Funded Employment Support

1.2 Step Ahead company records – all records including:

- HR
- Finance
- Governance
- Strategy, performance and audit
- Legal services
- Marketing
- Technology
- Health and Safety
- Environmental

Records not sent for central archive will be held within relevant areas for the appropriate retention period. Document owners should determine how records will be retained, and this must be recorded on the retention schedule.

2. Preparing electronic records for archive

All electronic records must be suitably prepared prior to being sent for archiving. This includes:

- The removal of duplicate data.
- The removal of any data that does not fall under the records retention schedules and which should not therefore be archived. The retention of unnecessary data could potentially be a breach of data protection legislation (e.g., if the records relate to personal data).

3. Archiving electronic records

Electronic records can be at risk of loss/damage if not managed appropriately. Portable storage devices are not intended for long-term storage or preservation of digital records. They are short-term storage solutions and should be used with caution. Regular and frequent changes in Information Technology mean that the currency or lifespan of certain technologies should be considered when sending electronic records for archive. Wherever possible, electronic records should be saved on Step Ahead's network which is backed up regularly. Under no circumstances should data be saved on any unapproved Cloud-based platforms or on a computer's hard drive/desktop.

4. Email Retention and Archiving

Emails that constitute, form part of, or support business records are classified as electronic records and must be managed in accordance with the Records Retention Schedule, as well as any applicable statutory, regulatory, funding, legal, or contractual retention requirements.

Emails that form part of official records must not be permanently deleted while they remain subject to retention requirements. All such emails must be stored using the approved Outlook archive function (or equivalent approved organisational archiving system), which constitutes the system of record for retained email correspondence.

Deletion of emails from inbox or mailbox systems is strictly limited to:

- Spam or junk communications
- Non-business-related correspondence
- Duplicate copies where a retained version exists in an approved archive

and only where this does not conflict with any legal, regulatory, funding, or contractual obligation.

Email inboxes must not be used as a primary or long-term storage location for business records. The archived system is the authoritative record for audit, compliance, and retention purposes.

Staff are responsible for ensuring emails are correctly classified and stored in the appropriate system. Non-compliance may result in breach of legal, regulatory, or contractual obligations.

5. Disposal of records

When records have reached their retention period, data will be disposed of securely and confidentially. The confidential destruction of records is a crucial element of good records management practice. It is a requirement of data protection legislation that all information relating to identifiable, living individuals is disposed of in an appropriately secure manner. Material that falls under any of the following categories needs to be treated as confidential:

- Records containing personal information (for example application/registration forms, assessments, payroll and pensions records, completed questionnaires, staff files, etc.)
- Records of a commercially sensitive nature (for example contracts, tenders, purchasing records, legal and financial documents)
- Records concerning intellectual property rights (for example unpublished data, draft papers and reports).

Heads and Managers are responsible for ensuring that their respective teams sort through and dispose of redundant electronic records in accordance with a records retention schedule. All documents are stored in such a manner as to be safe, and access to such material is controlled to ensure the confidentiality of personal data and always kept separately and securely with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Electronic data records and documents are stored in a manner that meets accepted security standards and legal requirements, ensuring they can be relied upon for audit purposes. Our appointed IT service company hosts our services on their own cloud infrastructure (EU-based); provider infrastructure is over two Data Centres, and they and their cloud infrastructure partner are accredited and certified. Data is backed up at regular intervals, ensuring speedy restoration of services/data supporting business continuity in any disaster recovery situation. The Microsoft Azure platform is totally secure and compliant, meeting international and industry-specific compliance standards.

All data is protected behind access control, requiring a unique account to access any information. All data is encrypted, including during storage and transmission. All data has an off-line backup with encryption. Accessing backups requires a unique account and completion of multi-factor authentication (MFA). All backups are managed through Acronis Cloud.

6. Backup Retention and Archive Distinction

Backups are retained strictly for business continuity and disaster recovery purposes and are not considered part of the formal records archive. Backups are not to be used as a substitute for archived or retained records and will be managed in accordance with defined backup retention schedules.

7. Incident / Data Loss Handling

Any loss, corruption, unauthorised deletion, or suspected compromise of records must be reported immediately in line with Step Ahead's incident reporting procedures. Appropriate corrective, investigative, and where necessary regulatory reporting actions will be undertaken.

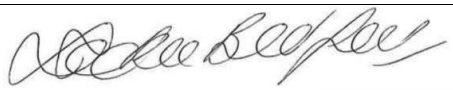
8. Roles and Responsibilities

Overall responsibility for records governance sits with Corporate Support, with operational responsibility delegated to document owners, Heads of Service, and Managers. All staff are responsible for ensuring compliance with this policy in their day-to-day handling of records. Subcontractors must comply with equivalent standards under contractual obligation.

9. Subcontractor and Third-Party Compliance

Where third-party providers or subcontractors process, store, or manage Step Ahead records, contractual agreements must ensure compliance with equivalent retention, security, and disposal standards, including GDPR Article 28 requirements where applicable. Compliance will be subject to periodic review or assurance checks.

Document Control	
Document Title: Document Retention Policy & Procedure	
Version Number: 1.7	Document Owner: Corporate Support
Date Approved: 30 June 2025	Approved By: Jackie Bedford, CEO

Effective Date: 30 June 2025 Superseded Version: 1.6	
Date of Last Review: 5 May 2026	Date of Next Review: 1 May 2026