DOCUMENT RETENTION POLICY AND PROCEDURE

BACKGROUND

Data Protection legislation (Data Protection Act 1998 and the General Data Protection Regulations (GDPR) from 25th May 2018) also contains requirements that impact on records retention namely, the requirement that personal data should not be retained for excessive periods and that data must be stored and disposed of securely.

The retention periods for many financial/legal documents must be clear in order to comply with mandatory requirements of external organisations such as HM Revenue and Customs and funding providers, namely Education and Skills Funding Agency (ESFA) and European Social Fund (ESF).

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 the only records that are retained are those defined in this schedule; in the context of this and the requirement to manage records for legislative purposes, Step Ahead therefore needs to consider and re-affirm its requirements and procedures for records retention. All appointed subcontractors are required to meet their legal and funding requirements and adhere to this policy.

DOCUMENT PURPOSE

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 such 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 including paper, microfilm, electronic records held on magnetic or digital media and photographic materials.

The records retention schedule is based on the guidance published by ESFA and ESF guidance July 2018.

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 papers (agenda, minutes, etc)

Retention and disposal schedules and procedures should, as 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.

RECORDS RETENTION SCHEDULE

Step Ahead's retention schedule is based on published ESFA and ESF guidance and 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 Head of HR and Corporate Support.

PROCEDURES

1. Archiving of paper records

1.1 Participant records are limited to documents relating to:

- Participant Data
- Funded Educational Support
- Funded Employment Support

1.1.1 ESF project evidence classed as core documentation that must be retained include:

- all ESF related documentation including work carried out during the development, pre application, application and during and after the project;
- the Funding Agreement including any revised versions supported by appropriate correspondence from DWP of the approval of changes to the Funding Agreement;
- correspondence from/to the Managing Authority;
- quarterly or monthly claim forms;
- working papers showing how claims were calculated, including any flat rate methodologies;
- the audit trail for all procurement undertaken for the project; and
- the State Aid approved scheme used where relevant.

N.B. It should be noted that all funded participant records need to be retained until at least 31st December 2030 for ESF funding from 2014-2022 and noting that retention is stated as 10 years after their final ESF claim is paid by the ESF Managing Authority. This is because ESF funding rules require these retention timelines to be adhered to.

1.2 Step Ahead company records – all records including:

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

For clarity under ESF projects the guidance states Step Ahead must keep records of the following things (although this list is not exhaustive):

- evidence of all project expenditure including invoices and bank statements or equivalent to show the payments were made;
- where indirect overheads costs and salaries have been apportioned to the project, records must show the agreed methodology for calculating these costs;
- records of eligible participants and any supporting evidence to confirm their eligibility to receive ESF support;
- evidence of open and fair procurement of goods and services including proof of advertising and contract notices, quotations or tenders received, and the scoring methodology used for selecting the successful candidate. This will include details of all preparatory work prior to the procurement process and the delivery/use of the procured service and goods.
- evidence of auditable, accountable match funding, including copies of match funding acceptance letters and bank statements showing receipt of match funding;
- compliance with publicity requirements. Copies of all publicity materials, including press releases and marketing must be retained to demonstrate the correct use of the EU logo and required text.
- compliance with equal opportunities and environmental sustainability requirements;
- clear records of businesses supported for state aid purposes, including signed declarations where an organisation is operating under any state aid rules, such as de minimis, or any other state aid ruling;
- documentary evidence substantiating the outputs and results declared in ESF claims and on completion of projects;
- a record of the identity and location of all bodies holding the supporting ESF project documentation and make this available on request to the Managing and Audit Authorities

Records which are not sent for central archive will be held within relevant areas for the appropriate retention period. It should be noted that it is not good practice to retain both paper and electronic records. Document owners should therefore

determine how records will be retained and this must be recorded on the retention schedule.

2. Preparing paper records for archive

All paper records must be suitably prepared prior to the data being sent for archiving.

This includes the following activities:

- 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 is costly and could potentially be a breach of data protection legislation e.g. if the records relate to personal data.
- The removal of all plastic wallets, sleeves and box files. This aids the destruction process at the end of the archiving period as all paper records can then be sent for confidential destruction without further intervention.
- The collation and securing of loose data
- Keeping a record within the area of what has been sent for archiving

All records must be placed in archiving wallets, boxed up and clearly marked with the following information using the approved wallet labels:

- Record type (see 1.1 for details)
- Subheading giving further information about the records e.g. programme area, alpha order details etc.
- Academic year the records relate to
- Name of funder and project title including contract number
- Destruction date

Records/documents with different destruction years must not be stored in the same wallet. All company records under heading 1.2 must be placed in archiving boxes and clearly labelled with two archiving box labels (the template can be found on the intranet). Boxes must not be overfilled. One label must be taped to the top of each box and the other to one of the short sides for the box. Boxes must then be sent to the appropriate Head of HR and Corporate Support for appropriate storage.

Any data which does not fall under the categories detailed in 1.1 and 1.2 or which has not been prepared and/or labelled correctly, will not be accepted for archiving. Areas will work on archiving annually during admin week in July. This means that all records to be sent for archiving will be managed in accordance with this procedure. All records to be disposed of will be removed from the archiving facility and disposed of via a confidential waste disposal service as detailed in section 4.

The Head of HR and Corporate Support will oversee this operation for all participant and company records. All records will be recorded on the appropriate archiving spreadsheet.

3. Archiving electronic records

Electronic records, like paper records, can be at risk of loss/damage is they are not managed appropriately. Portable storage devices like CD-ROMS, DVDs and USB drives are not intended for long-term storage or perseveration 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 personal data be saved on any unapproved Cloud based platforms or on a computer's hard drive/desktop.

4. 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).
- Material not classified as confidential may be disposed of via approved waste disposal services.

On an annual basis (usually in July to align with the academic year) Heads and Managers, are responsible for ensuring that their respective teams' sort through and dispose of redundant electronic records in accordance with the records retention schedule.

All documents are stored in such a manner as to be safe and that access to such material is controlled to ensure the confidentiality of personal data and always kept separately and securely, in lockable, fireproof, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Our appointed document management & storage service provider is Box-It, used by local government and compliant with ISO accredited procedures with 24 sites across London and the South East, include secure document storage and archiving, instant record retrieval, and collection and delivery of documents within 24 hours. We utilise

their online document management service which allows us to trace, track and request files from storage, and comprehensive audit tracking ensure full compliance with ESF and data protection legislation.

Electronic data records and documents are stored in secure off-site cloud-based servers that meet accepted security standards and legal requirements so can be relied upon for audit purposes. Appointed IT service companies host our services on their own cloud infrastructure (EU-based); provider infrastructure is over two DataCentres and they and their cloud infrastructure partner are ISO27001 accredited and are G-Gloud Certified and data is backed up via hourly snapshots ensuring speedy restoration of services/data supporting business continuity in any disaster recovery situation. Microsoft Azure platform is total secure and compliant meeting numerous international and industry-specific compliance standards (including ISO 27001) with security and privacy embedded into development, transparency over how our data is stored and accessed.

Revision Control

Date	Version	Overview of amendment(s)	Amendment date	Approved by	Approved date
11/07/2019	1.1	Reviewed for ESF compliance and addition of clause 1.1.1 and core document details under clause 1.2 of required documents	11/07/2019	Jackie Bedford (CEO)	12/07/2019

Approved and endorsed by:

Signed: 

Name: Jackie Bedford

Title: Chief Executive

Date: 12th July 2019