Document Retention Policy v3

This policy:

- Applies to all colleagues, volunteers, agency workers and those providing services under a contract or other agreement (referred to within this policy as "workers").
- Replaces the Document Retention Policy (last reviewed July 2018)
- In compliance with the No Life Half Lived Strategy: *"To be effective and accountable in all that we do."*
- Does not form part of any contract or agreement and we may amend it at any time.

In line with our commitment to equal opportunities, this policy can be made available in a variety of formats, including large print, translated into another language or other media. Reasonable adjustments will also be made to assist individuals who have a disability.

We will endeavour to develop fair and consistent policies, procedures and practices to support our aims, values and objectives.

1. Our Human Rights Approach

1.1 We recognise everyone's individual rights and freedoms. They are based on important principles such as dignity, fairness, respect and equality.

1.2 In developing a human-rights based approach, this means that colleagues, volunteers, agency workers, service users and peer support groups have been fully supported to participate in the development of this policy.

2. Our Values

2.1 Our values are at the heart of what we do. We also recognise that people are the most important asset in achieving No Life Half Lived in Scotland.

3. Statement of Intent

3.1 The corporate information, records and data of CHSS is important to how we conduct business and manage colleagues.

3.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. We also retain data to help our organisation operate and to have information available when we need it. However, we do not need to retain all data indefinitely, and retaining data can expose us to risk as well as be a cost to our business.

3.3 The purpose of this policy is to detail the procedures for the retention and disposal of data to ensure that we carry this out consistently and that we fully document any actions taken. This retention and disposal policy refers to physical data, such as hard copy documents, contracts, notebooks (including handwritten notes, post-its etc.), letters and invoices, and digital data such as databases, data files, emails, digital documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

3.4 This policy also covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by colleagues on CHSS devices (Note: it is forbidden to store CHSS data on personal devices or otherwise remove it from CHSS authorised systems; if it is beyond CHSS direct control, it is considered non-compliant with our duties under UK General Data Protection Regulations).

3.5 This policy explains the differences between our formal or official records, disposable information, confidential information belonging to others, personal data and non-personal data. It also gives guidance on how we classify our data.

3.6 This policy should be read in conjunction with the following documents:

- People Policy on Confidentiality & Data Protection
- Privacy Notice
- Employment Records: Retention and Erasure Guidelines

3.7 This policy is intended to ensure that we process personal data in the form of employment records in accordance with the personal data protection principles, in particular that:

- Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
- Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.
- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When personal data is no longer needed for specified purposes, it is deleted or anonymised as provided by this policy. Anonymised data must not be able to be combined with freely available data which can then be used to identify the individual. For example, Electoral Register or social media profiles.
- Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate or as a Data Subject request.
- Personal Data must be secured by appropriate technical and organisational measures against unauthorised use / intrusion or unlawful processing, and against accidental loss, destruction or damage.

3.8 The Data Protection Officer (DPO) is responsible for advising on and monitoring our compliance with data protection laws which regulate personal data and overseeing this policy. Our DPO works with individual Directors on the retention requirements for personal data and on monitoring compliance with this policy in relation to personal data for each Department. Any questions about the operation of this policy should be submitted to the DPO, who is Rachel Ducker, Director of Finance & ICT.

3.9 Failure to comply with this policy can expose CHSS to fines and penalties as the registered Data Controller, adverse publicity, difficulties in providing evidence when we need it and in running our business. In some instances, it can also result in criminal penalties.

4. General Principles

4.1 Our approach to retaining records is to ensure that it complies with the data protection principles referred to in this policy (See appendix 1).

4.2 In particular, we aim to ensure that:

- Records are regularly reviewed to ensure that they remain adequate, relevant and limited to what is necessary.
- Records are kept secure and are protected against unauthorised access / intrusion or unlawful processing and against accidental loss, destruction or damage.
- When records are destroyed, whether held as paper records or in digital format, We will ensure that they are safely and permanently erased.

4.3 Our Privacy Notice advises individuals how long we expect to keep their personal data for. This will vary from department to department.

4.4 Data, in both paper and digital form, will be held by the relevant Department. Each Department will hold a data retention register of data held (manual and digital) and the retention/erasure timescale that applies. Destruction of data will take place in accordance with this register.

4.5 No data should be retained on anyone's personal drive or personal (i.e non-CHSS device.

4.6 We expect everyone to destroy data as follows:

- Personal data – Securely shredded.
- Sensitive personal data – Securely shredded.
- Digital data, including data in:
  - CHSS devices (computer, laptop, mobile etc.)
  - CHSS Networks (the H: drive for example)
  - Teams
  - SharePoint
  - OneDrive
  - Outlook (emails and attachments)
  - other digital systems such as Databases, websites, apps, spreadsheets, data files, backups etc

4.7 Guidance should be sought from the ICT Team about these issues to ensure compliance.

4.8 All colleagues and approved third party data processors must comply with this policy, the Document Retention Guidelines, any communications suspending data disposal and any specific instructions from the relevant Director or Head of/Senior Manager. Failure to do so

may subject CHSS, our colleagues, and contractors to serious civil and/or criminal liability.

5. Types of Data and Data Classifications

5.1 **Formal or official records**. Certain data is more important to us and is therefore listed in the Document Retention Guidelines. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see paragraph 0 below for more information on retention periods for this type of data.

5.2 **Disposable information**. Disposable information consists of data that may be discarded or deleted at the discretion of the colleague once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy and the Document Retention Guidelines. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of CHSS and retained primarily for reference purposes.
- Spam and junk mail.

Please see paragraph 5.3 below for more information on how to determine retention periods for this type of data.

5.3 **Personal data.** Both formal or official records and disposable information may contain personal data; that is, data that identifies living individuals. Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (See Appendix 1 for UK GDPR Principles, Article 5(1)(d)). See paragraph 5.4 below for more information on this.

5.4 **Confidential information belonging to others**. Any confidential information that a colleague may have obtained from a source outside of CHSS, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. We will return unsolicited confidential information to the sender where possible, and delete, if received.

5.5 **Data classifications.** Some of our data is more confidential than other data. Our People Policy on Confidentiality and Data Protection explains how we classify data and how each type of data should be marked and protected. When complying with this policy, it is also important that you follow our People Policy on Confidentiality and Data Protection.

6. Retention Periods

6.1 Formal or official records. Any data that is part of any of the categories listed in the Document Retention Guidelines (see Appendix 2), must be retained for the amount of time indicated in the Document Retention Guidelines. A record must not be retained beyond the period indicated in the Document Retention Guidelines, unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the DPO.

6.2 **Disposable information.** The Document Retention Guidelines will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

6.3 **Personal data.** As explained above, UK GDPR requires us to retain personal data for no longer than is necessary for the purposes for which it is processed. Where data is listed in the Document Retention Guidelines, we have taken into account the UK GDPR principles and balanced this against our requirements to retain the data. Where data is disposable information, you must take into account the requirement for retention no longer than is necessary when deciding whether to retain this data. More information can be found in in our People Policy on Confidentiality and Data Protection.

6.4 **What to do if data is not listed in the Document Retention Guidelines.** If data is not listed in the Document Retention Guidelines, it is likely that it should be classed as disposable information. However, if you consider that there is an omission in the Document Retention Guidelines, or if you are unsure, please contact the Data management team (data@chss.org.uk) for guidance.

7. Storage, Back-Up and Disposal of Data

7.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner. Any documents and financial files that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week and maintained off site. Backups for critical data systems may be hourly, for example medical records. Please contact the ICT Team for advice.

7.2 **Destruction**. Our Data Management Group is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and colleague-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of digital data must be co-ordinated with the ICT Team.

7.3 The destruction of data must stop immediately upon notification from the Data Management Group that preservation of documents for contemplated litigation is required (sometimes referred to as a litigation hold). This is because we may be involved in a legal claim or an official investigation (see section 8 below). Destruction may begin again once the Data Management Group lifts the requirement for preservation.

8. Special Circumstances

8.1 **Preservation of documents for contemplated litigation and other special situations.** We require all colleagues to comply fully with our Document Retention Guidelines and procedures as provided in this policy. All colleagues should note the following general exception to any stated destruction schedule: If you believe, or the Data Management Group informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other digital documents, until the Data Management Group determines those records are no longer needed. Preserving documents includes suspending any requirements in the Document Retention Guidelines and preserving the integrity of the digital files or other format in which the records are kept.

8.2 If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Data Management Group.

8.3 In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as our merger with another organisation or the replacement of our information technology systems.

9. Breach of this Policy

9.1 If you suspect a breach has occurred, you should either discuss it with your Line Manager for guidance or initiate the Data Protection Reporting Procedure for a formal investigation to take place. The breach should also be reported to the Rachel Ducker our Data Protection Officer (rachel.ducker@chss.org.uk) who will determine whether this is a reportable incident to the Information Commissioner. In addition, formal action may be taken against the individual.

9.2 For formal/informal guidance or advice, you can contact the Head of ICT at icthelpdesk@chss.org.uk, who can help you assess if there is indeed a reportable incident or assist you in managing an issue.

10. Responsibilities

10.1 Each Department will have retention periods for holding personal data in compliance with our People Policy on Confidentiality and Data Protection and the UK General Data Protection Regulations. Each Director is responsible for ensuring:

- Departmental data retention register's timescales are adhered to.
- Data retention register is recorded on SharePoint.

10.2 All colleagues (and those outlined at the start of this policy) will comply with this policy and undertake any compliance training in GDPR, Cyber Security or other training identified.

10.3 We have designated the Head of ICT as the Records Management Officer. The Records Management Officer will chair the Data Management Group and is responsible for:

- Administering the data management programme;
- Helping department heads implement the data management programme and related best practices;
- Planning, developing, and prescribing data disposal policies, systems, standards, and procedures; and
- Providing guidance, training, monitoring and updating this policy.

10.4 The Director of Finance, Director of People Driven Development, Head of ICT and Head of People are available to give advice and interpretation to you on any aspect of this policy. The ICT Team can advise and offer support on digital or technical issues, both formally and informally.

10.5 The Audit & Compliance Lead will ensure policy compliance through regular departmental audits. Where relevant, the Audit & Compliance Lead will report any breach, reviewing the risk management register, where relevant.

10.6 The above named will, in conjunction with the relevant Director, oversee any complaints received in respect of this policy, including rectification or reporting to the Information Commissioner.

12. Monitoring and Review

12.1 The Data Management Group will monitor the effectiveness of this policy.

12.2 The Audit & Compliance will report any breaches of this policy to the Directors' Group and Audit and Risk Committee .

12.3 The Director of People Driven Development will report any serious (as outlined in section 9.1 above) breaches to the Staff Governance Committee on a quarterly basis.

12.4 This policy will be reviewed 3 years or earlier if deemed appropriate. In the event that this policy is not reviewed within the above timescale, the latest approved policy will continue to apply.

Appendix 1: UK GDPR Principles

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:
"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Appendix 2: Document Retention Guidelines

These guidelines list reasonable time periods recommended for retaining records.

Accident reports and claims (settled cases) -- 7 years
Accommodation requests -- 1 year after record is made
Accounts payable ledgers and schedules -- 7 years
Accounts receivable ledgers and schedules -- 7 years
Ads & Notices of overtime opportunities -- 1 year after record is made
Ads & Notices of promotion opportunities -- 1 year after record is made
Age certificates (minors only) -- Duration of employment
Apprenticeship program records -- 2 years (records made solely for completing Form EEO-2 or similar reports must be kept for one year from date of report)
Aptitude tests -- 1 year from personnel action to which test relates
Audit reports of accountants -- Indefinitely
Bank reconciliations -- 1 year
Bank statements -- 7 years
Basic colleague information -- 4 years after termination
Basic payroll information -- 3 years after record is made
Capital stock & bond records -- Indefinitely
Cash books -- Indefinitely
Certificates and notices of Wage and Hour Administrator -- 3 years after record is made
Charts of accounts -- Indefinitely
Cheques (canceled, see exceptions below) -- 7 years
Cheques (canceled for important payments, i.e., taxes, purchases of property, special contracts, etc.) -- Indefinitely
Collective bargaining agreements -- 3 years from end of agreement
Construction documents -- Indefinitely
Contracts and leases (expired) -- 7 years
Contracts and leases still in effect -- Expiration + 7 years
Correspondence (general) -- 3 years
Correspondence (legal or important) -- Indefinitely
Dates FMLA leave is taken -- 3 years from end of leave
Demotion records -- 1 year from date of action
Depreciation schedules -- Indefinitely
Duplicate deposit slips -- 1 year
EEOC Records -- Until final disposition of the charge
Electronic fund transfer documents -- 7 years
Colleague benefits plan records -- Duration of plan plus one year
Employment contracts -- Expiration + 7 years
Ex-colleague personnel records -- 7 years

Employment applications (regular) -- 3 years
Expense analyses and expense distribution schedules -- 7 years
Exposure records -- Duration of employment plus 30 years
Financial statements (end-of-year, other months optional) -- Indefinitely
Form EEO-1 -- As long as current
General and private ledgers (and end-of-year trial balance) -- Indefinitely
Hours of FMLA Leave -- 3 years after leave ends
Hours worked in tipped & non-tipped positions -- 3 years after record is made
Job advertisements -- 1 year after record is made
Job requests given to employment agencies -- 1 year from time of request
I-9s (after termination) -- 1 year
Insurance policies (expired) -- 3 years
Inventories of products, materials, supplies -- 7 years
Invoices to customers -- 7 years
Invoices from vendors -- 7 years
Journals -- Indefinitely
Layoff, reduction-in-force, & recall records -- 1 year from date of action
Licenses -- Indefinitely
Loan documents, notes -- Indefinitely
Medical certifications -- 3 years from date record is made
Medical examinations -- 1 year after termination (Note: OSHA says legally-required exams must be kept for 30 years after termination.)
Merit, incentive system records -- 2 years from date records is made
Minute books of directors and stockholders, including by-laws and charter -- Indefinitely
Notes receivable ledgers and schedules -- 7 years
Notices of FMLA leave -- 3 years from end of leave
OSHA Form (Log and Summary of Occupational Injuries & Illnesses) -- 5 years
Option records (expired) -- 7 years
Payroll records and summaries, pensions, payroll taxes -- 7 years
Petty cash vouchers -- 3 years
Personality tests -- 1 year from personnel action to which tests relates
Personnel records -- 1 year from making the record
Physical exams -- 1 year from personnel action to which test relates
Physical inventory tags -- 3 years
Plant cost ledgers -- 7 years
Pre-employment tests -- 1 year from date of test
Premium payments of colleague benefits -- 3 years from end of FMLA Leave
Promotion records -- 1 year from date of action
Property records -- Indefinitely
Property appraisals by outside appraisers -- Indefinitely
Property records including costs, depreciation reserves, end-of-year trial balances, depreciation schedules, blueprints and plans -- Indefinitely

Purchase orders (yours) -- 1 years
Purchase orders (theirs) -- 7 years
Rates of pay -- 1 year after record is made
Records of disputes and about designation of FMLA Leave -- 3 years
References -- 1 year after record is made
Resumes (after termination) -- 1 year
Resumes (unsolicited) -- Return to sender immediately*
Receiving sheets -- 1 year
Requisitions -- 1 year
Sales records -- 7 years
Scrap and salvage records (inventories, sales, etc.) -- 7 years
Subsidiary ledgers -- 7 years
Summary Plan Description data -- 6 years
Supplementary payroll data -- 2 years after record is made
Steno notebooks/word-processor files/disks -- 1 year**
Tax returns and worksheets, reports, documents relating to income tax liability -- Indefinitely
Time books/cards (for exempt & non-exempt colleagues) -- 7 years
Time cards/sheets -- 3 years after record is made
Tips reported by colleagues -- 4 years from the later of tax due date or payment date
Total wages paid to each colleague -- 4 years from later of tax due date or payment date
Track & Trace (Covid-19) Records – 14 days from the day of visiting CHSS premises
Trademark registrations -- Indefinitely
Training selection records -- 1 year
Transfer records -- 1 year from date of action
Voucher register and schedules -- 7 years
Vouchers for payments to vendors, colleagues (including allowances and reimbursement of colleagues, officers, for travel and entertainment expenses) -- 7 years
W-4 forms -- 4 years
Welfare & pension reports -- 6 years
Worker's' comp. documents -- 11 years
Written training agreements -- Duration of training program