

Cambridge House Data Retention Policy



Contents

1.	Purpose, Scope and Users	2
2.	Reference Documents	3
3.	Retention Rules	3
3.1.	Retention General Principle.....	3
3.2.	Retention General Schedule.....	3
3.3.	Safeguarding of Data during Retention Period	4
3.4.	Destruction of Data.....	4
3.5.	Breach, Enforcement and Compliance.....	4
4.	Document Disposal	5
4.1.	Routine Disposal Schedule.....	5
4.2.	Destruction Method	5
5.	Managing Records Kept on the Basis of this Document	6
6.	Validity and document management	6
	Appendix A	7
	Communication Activities	7
	Corporate (non-GDPR)	7
	Governance (non-GDPR).....	8
	Finance (non-GDPR)	8
	Fundraising and Development (non-GDPR)	8
	Human Resources	9
	Service Users	9

1. Purpose, Scope and Users

- a) This policy sets out the general principles of data retention and the specific retention periods for categories of personal data and sets out the minimum standards to be applied when destroying, anonymising or archiving certain information. Data should only be kept for as long as there is an administrative need to keep it to carry out its business or support functions, or for as long as it is required to demonstrate compliance for audit purposes or for legislative requirements. Where documents are not personal data they should be kept in line with the legal or contractual requirements that led to their production e.g. contract performance reports should not significantly outlive the contract they serve.
- b) This Policy applies to all business services, processes and systems in any countries in which Cambridge House and Talbot conducts business and has dealings or other business relationships with third parties.
- c) Appendix A provides details for:
 - Communication activities
 - Corporate services
 - Governance activities
 - Finance
 - Fundraising and development
 - Human resources
 - Service users
- d) This Policy applies to all Company officers, directors, employees, volunteers, agents, affiliates, contractors, consultants, advisors or service providers that may collect, process, or have access to data (including personal data and / or sensitive personal data). It is the responsibility of all of the above to familiarise themselves with this Policy and ensure adequate compliance with it.
- e) This policy applies to all information used at Cambridge House and Talbot. Examples of documents include:
 - Emails
 - Hard copy documents
 - Soft copy documents
 - Video and audio
 - Data generated by physical access control systems and databases
- f) The Data Protection Officer (DPO) is a legal role which the Chief Executive will include in a staff member's job role or by amendment to a pre-existing job role. The DPOs assist the Chief Executive to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the information Commissioner's Office. The DPO is currently the Head of Administration and Corporate Services.

- g) **The Charities Act 2011 and The Charities (Protection and Social Investment) Act 2016:** This legislation sets out the function and responsibilities of charities and gives the legal basis for the Charity Commission. Under these laws, records may be required for the following:
- Preparation of Annual Reports
 - Preparation of the annual submission to the Charity Commission (including financial data)
 - Demonstrating to the Charity Commission (amongst others) that the organisation is well-run and has suitable governance arrangements
 - To provide evidence to the Charity Commission in the event of an enquiry into the charity – this could mean any information which Commissioners deem to be relevant.

Charities have a legal duty to comply with requests for information from the Charity Commission, and the Commission expects this information to be readily available. If information is not available, the Commission has the power to ask why. One defence afforded to charities is that records have been securely destroyed according to a disposal policy. However, organisations would be wise to err on the side of caution when deciding what to dispose of.

2. Reference Documents

- a) The EU GDPR is an EU Regulation and it no longer applies to the UK. If you operate inside the UK, you need to comply with the Data Protection Act 2018 (DPA 2018). The provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations.
- b) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
- c) Cambridge House's Data Protection, Privacy and Confidential Policy; Fundraising and Communication Data Protection Policy; Clear Desk Policy; and Mutual non-disclosure agreement (template).

3. Retention Rules

3.1. Retention General Principle

In the event, for any category of documents not specifically defined elsewhere in this Policy (and in particular within the Data Retention Schedule), the Head of Service will define the retention length in consultation with the Data Protection Officer. The Head of Service will consider on what basis the data was collected and for how long that data needs to be retained to carry out business or support functions, or for as long as it is required to demonstrate compliance for audit purposes or for legislative requirements. If we do not need to identify individuals, the data should be anonymised so that identification is no longer possible.

3.2. Retention General Schedule

The Data Protection Officer will maintain the Data Retention Schedule in consultation with colleagues.

As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from other authorities, if there is a chance records of personal data are needed by Cambridge House and Talbot to prove compliance with any legal requirements;
- When exercising legal rights in cases of lawsuits or similar court proceedings recognised under local law.

3.3. Safeguarding of Data during Retention Period

Most data is now digital but for clarity Cambridge House has a clear desk policy, and all working files/documents should be stored in lockers when not being worked on. As soon as possible documents should be scanned and uploaded to the appropriate database (usually Advice Pro/MS Teams) where appropriate safeguards are in place. The responsibility for the storage falls to the Data Protection Officer.

3.4. Destruction of Data

Cambridge House and Talbot and its employees should therefore, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See **Appendix A** for the retention schedule. Overall responsibility for ensuring the correct method for destruction of data falls to the DPO.

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. In some circumstances it may be preferable to anonymise the data. Fully 'anonymised' data does not meet the criteria necessary to qualify as personal data and is therefore not subject to the same restrictions placed on the processing of personal data under the UK GDPR. Data can be considered 'anonymised' when individuals are no longer identifiable. The **Document Disposal Schedule section below defines the mode of disposal.**

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the DPO has agreed can be subcontracted for this purpose. Any applicable general provisions under relevant data protection laws and Cambridge House and Talbot's Personal Data Protection and Privacy Policy shall be complied with.

The DPO shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

3.5. Breach, Enforcement and Compliance

- a) The Data Protection Officer has the responsibility to ensure that each of Cambridge House and Talbot's service areas comply with this Policy. It is also the responsibility of the DPO to assist with enquiries from any local data protection or governmental authority.
- b) Any suspicion of a breach of this Policy must be reported immediately to DPO. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

c) Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of Funder confidence, litigation and loss of competitive advantage, financial loss and damage to Cambridge House and Talbot's reputation, personal injury, harm or loss. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to Company premises or information, may therefore result in disciplinary proceedings which could lead to termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

4. Document Disposal

4.1. Routine Disposal Schedule

- a) Personal data must be information that relates to an individual. That individual must be identified or identifiable either directly or indirectly from one or more identifiers or from factors specific to the individual. Data that doesn't fall into this category can be routinely destroyed by via confidential waste or shredding. This can include:
- Reservations for internal meetings without charges / external costs;
 - Requests for ordinary information such as travel directions
 - Transmission documents such as letters, fax cover sheets, e-mail messages, routing slips, compliments slips and similar items that accompany documents but do not add any value; Message slips;
 - Superseded address list, distribution lists etc.;
 - Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases.
 - Stock in-house publications which are obsolete or superseded;
 - Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organisations.

4.2. Destruction Method

- a) **High risk** documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (placed into locked bins for collection by an approved disposal company) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction. High risk documents contain the following information, although the list is not exhaustive:
- | | |
|--------------------------|---|
| ▪ Race and ethnic origin | ▪ biometrics (where used for ID purposes) |
| ▪ politics | ▪ health |
| ▪ religion | ▪ sexual Orientation |
| ▪ trade union membership | ▪ banking details |
| ▪ genetics | ▪ home address/personal contact details |

- b) **Medium risk** documents are proprietary documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data. The documents should be placed into locked bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.
- c) **Low risk** documents are those that do not contain any confidential information or personal data and are published Company documents. These should be shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

5. Managing Records Kept on the Basis of this Document

Record name	Storage location	Person Responsible for storage	Controls for record protection	Retention time
Data Retention Schedule	<ul style="list-style-type: none"> ▪ Data Protection Officer's One Drive. Staff policy and procedure library on shared drive. ▪ CH Office 365 SharePoint 	Data Protection Officer	Read access only available to all CH staff, volunteers, directors and officers	Permanently

6. Validity and document management

- a) The current DPO is the Head of Administration and Corporate Services
- b) This document is valid as of The owner of this document is the DPO who must check and, if necessary, update the document at least once a year.

Appendix A

Communication Activities

	Retention Trigger	Retain for	Action	Retention source	Officer responsible
Staff mailbox and Outlook	Creation	3 years	Archive	Business need	Employee
Scanned documents	Once Scanned	1 Month	Destroy	Business need	
Internal email	Creation	3 years	Archive	Business need	
External email	Creation	3 years	Archive	Business need	
Text Messages (CH mobile phone users)	Creation	1 year	Delete	Business need	

Corporate (non-GDPR)

	Retention Trigger	Retain for	Action	Retention source	Officer responsible
H&S Inspections, Property Management and Asset records	Last Action	7 years	Review	The National Archives Retention Scheduling. H&S at work act 1974. Limitation act 1980	Head of Administration and Corporate Services
Documents relating to IT system integral to their running and long-term use	When initially Created or received by service provider	7 years	Review	Business need	
IT Infrastructure	Last Action	7 years	Review	Business need	
Information security	Last Action	7 years	Review	Business need	
Information requests		7 years	Destroy	Business need	
Legal advice	Last action	7 years	Review	Business need	Chief Executive and Head of Administration and Corporate Services
Service Contracts	End of contract	7 years	Review	The National Archives Retention Scheduling	Head of Administration and Corporate Services
Residents License Agreements	End of contract	2 years	Destroy	Business need	

Governance (non-GDPR)

	Retention Trigger	Retain for	Action	Retention source	Officer responsible
Memorandum and Articles of Association	Creation	Permanently		Charity commission, FOI act and Business need	Chief Executive
Board and Sub Committee meeting minutes	Minutes Agreed	Permanently	Archive	Charity commission	Chief Executive
Corporate Governance Support	Last Action	7 Years	Review	Business need	Chief Executive
Organisation wide corporate plans, policies, Business Contingency, Risk Management and Business strategies	Superseded	7 years	Review	Business need	Chief Executive
Corporate Roles and Responsibilities	Superseded	7 Years	Review	Business need	Chief Executive
Data Protection and FOI complaints	Closure	7 years	Destroy	Business need	Head of Administration and Corporate Services
Audits reports	Closure	7 years	Review	Business need	Finance Director
Data Breach reports	Closure	7 Years	Destroy	Business need	Head of Administration and Corporate Services
Insurance: public liability, employers' liability, Personal Indemnity	Creation	Permanently	Archive	National Archives retention scheduling	Head of Administration and Corporate Services

Finance (non-GDPR)

	Retention Trigger	Retain for	Action	Retention source	Officer responsible
Financial Information	End of financial year	7 years	Destroy	HM Treasury guidelines, National audit office advice, Companies Act	Finance Director
Payroll Reports	End of financial year	7 years	Destroy	HM Treasury guidelines, National audit office advice, Companies Act	

Fundraising and Development (non-GDPR)

	Retention Trigger	Retain for	Action	Retention source	Officer responsible
Individual Donor information	Creation	7 years	Review	Business need, Fundraising regulator, Data protection Act	Fundraising and Development Coordinator
Fundraising participant information	Creation	7 years	Review	Business need, Fundraising regulator, Data protection Act	
Research Data	Creation	7 years	Review	Business need	
Seminar attendee lists	Creation	7 years	Destroy	Business need	
Online donation data	Creation	7 years	Review	Business need, Fundraising regulator, Data protection Act	

Human Resources

	Retention Trigger	Retain for	Action	Retention source	Officer responsible
Employee files, supervisory and Personal development records	End of employment	7 years	Destroy	National Archives Retention scheduling, and Employee Personnel Records	Chief Executive
Disciplinary and Grievance.	End of employment	7 years	Destroy	Limitation Act 1980	Chief Executive
Employment contracts and Job descriptions	End of employment	7 years	Destroy	Limitation Act 1980	Chief Executive
Payroll spreadsheet information	End of employment	7 years	Destroy	HM Treasury Guidelines and National Archives Retention Scheduling	Finance Director
Maternity, Paternity Adoption and Sick leave	End of employment	3 years	Destroy	SSP regulations 1982 (general) SMP regulations 1986 (general) and statutory Adoption pay 2002 (administration)	Chief Executive
Successful recruitment candidate information, (including third party referee details provided by the applicant)	End of employment	7 years	Destroy	The National archives retention scheduling	Chief Executive
Unsuccessful recruitment candidate information (including third party referee details provided by applicant)	Last Action	6 months	Destroy	Limitation act 1980	Heads of Service
Staff pension, pay history and termination reasons	From date of commencement	100 years	Destroy	National Archives Retention scheduling, and Employee Personnel Records	Chief Executive
Third party emergency contact details provided by staff	End of employment	Immediate	Destroy	Business need	Chief Executive
Equality and Diversity (Published information only)	Last Action	7 years	Review	Public sector equality duty	Chief Executive
Employee audits	Last Action	7 years	Review	Public sector equality duty	Chief Executive

Service Users

	Retention Trigger	Retain for	Action	Retention source	Officer responsible
Client Evaluation forms	Creation	7 years	Destroy	Business need	Heads of Services
Client Data/papers including carer details, case management, billing information	Creation	7 years	Destroy	Business need	
Complaints Records	Creation	7 years	Destroy	Business need	Head of Administration and Corporate Services
Photographic images and video footage.	Recorded	7 years	Destroy	Business need	Heads of Services
Client reports, case reviews	Case closed	7 years	Destroy	Business need	
Third party contact details: Solicitors, health and social care providers, friends and family, Landlords and Letting agents.	Creation	7 years	Destroy	Business need	
Records relating to Children	Creation	Until child reaches 21	Destroy	Limitation Act 1980	