Title of Document	**Record Management, Retention & Deletion Policy**
Name of Department	**Quality**

What type of document is this?	**Policy**		
Which Helping Hands POL/SOP does this document relate to?	Information Governance POL Data Protection Policy Information Security (Inc Cyber Security) POL Privacy Information POL Information Handling & Sharing POL Information and Data Sharing SOP Information Risk Management SOP Data Protection Impact Assessment SOP	**Index number of POL/SOP**	POL-084 POL-085 POL-082 POL-007 POL-086 SOP-039 SOP-040 SOP-038

Which Operational Priority/Priorities does this document link to?	Governance Framework	Internal & External Communications	Information Management & Technology

Custodian of document	Group Managing Director	**Committee responsible for this document**	Policy Committee
Approval date and committee chairperson signature	02.07.2025	**When is its next scheduled review?**	02.07.2028

Who does it apply to?	All Helping Hands staff at all facilities					
		Does it apply to bank workers?	Yes	**Does it apply to agency staff?**	NA	**Does it apply to third party contractors?**	NA

Purpose of the Policy	To ensure that archived personal and sensitive data approaching the end of their retention period is reviewed and deleted or destroyed securely. This Policy complies with UK GDPR storage limitation principle, the 'right to be forgotten' and Helping Hands Retention Schedule.

ROLES AND RESPONSIBILITIES

Role	Responsibility
Data Protection Officer (DPO) / GDPR Compliance	The DPO has overall responsibility to ensure all areas of the business complies with this policy. Initial contact point for senior management for final authorisation of deletion / destruction when applicable and to review / update this policy and retention schedule
Senior Leader Team **Directors** **Heads of Departments**	To ensure staff adherence with this policy and associated procedures in line with UK GDPR and Data Protection Laws Responsibility for review and authorising the deletion/destruction of records in line with this policy and retention schedule and retention of evidence of deletion/destruction
All Managers	Comply and adherence to this policy and the day to day records management, archiving and storage in line with UK GDPR and associated procedures
Employees	Comply and adhere to the GDPR principles and procedures in line with this policy and associated SOPs and Working Instructions where relevant. Responsible for day to day records management and ensuring the accuracy of information that is collected in a lawful, fair and transparent manner.

1. Scope

1.1. This policy provides employees with information and requirements related to management of records, the archiving of digital and paper records, and the review and destruction of records process.

2. Record Management

2.1. Record management is an administrative process that occurs throughout the life cycle of any data. Helping Hands adheres to GDPR principles to manage data and records. The life span of a record can be expressed into 5 phases:

- Record creation
- Record use (data processing)
- Record maintenance
- Record storage / archiving
- Record destruction / deletion

3. Record Creation

3.1. The content of a record will primarily be determined by the purpose for which it is being created, for example a personnel file will contain information about an employee relating to employment history, payroll details and training, or a customer file will contain information about the necessary care arrangements and support required to provide our core service.

3.2. Any information collected and subsequently used to create a record is done under a legal basis for processing as outlined in Helping Hands Privacy Notice which is available to view on the website. In addition to this legal requirement, it is important that any record created is:

3.2.1. Factual, consistent and accurate

3.2.2. Recorded and legible

3.2.3. Recorded as soon as possible after an event has occurred, providing current information

3.2.4. Recorded in such a way that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly

3.2.5. Accurately dated, timed and signed with the signature where appropriate

3.2.6. Reviewed periodically and amended to maintain the accuracy of the data

3.2.7. Not include abbreviations (unless officially accepted e.g. Clinical or Medical), jargon, meaningless phrases, irrelevant speculation and offensive subjective statements

3.2.8. When written it must be in black or blue ink, or as defined within the record, preferably using a ball point pen (fountain pen ink should be avoided as this will run if the record becomes wet) and dark enough that all writing is legible on any photocopies

3.2.9. Free from the use of any correctional fluid

4. Record Use

4.1. Records for use in business activities should be complete enough to:

4.1.1. Facilitate an audit or examination of the business by authorised individuals

4.1.2. Protect the legal and other rights of Helping Hands, its customers and any other person affected by its actions

4.1.3. Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative

5. Record Maintenance

5.1. Helping Hands collects different types of data ranging from employee records, care records, property records, communication records, training records, policy records, corporate records, legal, complaints and information rights records, financial and transaction records.

5.2. These records must be accurate, kept up to date and maintained by the relevant asset owners, individuals or departments and kept securely in paper or digital format. Efficient record maintenance is reliant on establishing and conducting regular reviews and auditing, and where it relates to records containing personal and sensitive data, employees must adhere to the GDPR principles (see Helping Hands Data Protection policy for principles).

5.3. The key consideration of any record management system is knowing what information a record contains and where it needs to be at any given point of the data life cycle.

5.3.1. Email records

5.3.1.1. Emails form an important part of the corporate records held by Helping Hands. Employees are responsible for managing their inboxes to ensure that emails of business value are filed properly, actioned where appropriate and can be found in a timely manner. As this only accounts for a small percentage, identifying the relevant emails to retain reduces the storage burden, reduces inefficiency and increases the risk of non-compliance.

5.3.1.2. Helping Hands IT Support manages the company email archiving systems and are responsible for email activation, deactivation and the storage of emails in line with the Helping Hands Retention Schedule. All requests for archived emails must be directed through to Senior Management for authorisation.

5.3.2. Digital Care records

5.3.2.1. Helping Hands has a clearly defined approach to monitor care records in use.

5.3.2.2. Records should be audited regularly in line with Helping Hands procedures (W.I-054 Auditing & Audit Tools) to ensure that all records kept are being monitored and maintained.

5.3.2.3. Helping Hands does not condone any individual that collects or absconds with any form of record or confidential documents belonging to a customer or the company; and who fails to return them to a secure and approved location in a timely manner. This action will be considered as intentional or deliberate misconduct and a data breach subject to disciplinary proceedings.

6. Records Storage and Archiving

6.1. Digital records

6.1.1. Records are digitally stored within record management applications.

6.1.2. Where customers cease care and employees cease employment with Helping Hands, records are archived within the respective record management applications.

6.2. Existing Paper Customer MAR and Visit Records

6.2.1. Records are stored at a secure and controlled offsite location.

6.2.2. A digital library is maintained to source relevant records (*see section 14.0 for record of Destruction of paper records).*

7. Records Retention

7.1. Helping Hands has a retention schedule (*Appendix One*) to maintain control of the various records that need to be kept. To determine the retention period, the following factors are considered and approved by the Data Protection Officer:

7.1.1. Any contractual obligations and rights in relation to the information provided

7.1.2. Legal obligation(s) under applicable law to retain data for a certain period of time

7.1.3. Statute of limitations under applicable law(s)

7.1.4. Adherence with relevant data protection authorities

7.1.5. Any requests by data subjects for the 'right to be forgotten'

7.1.6. Legitimate considerations and suggestions sought from different core business sectors dependant on the purpose of the record

7.1.7. The aim of the is to maximise the availability of the information for the effective conduct of the business whilst complying with specific legal and regulatory requirements.

7.1.8. The Helping Hands Retention Schedule (*Appendix One*) ensures that the destruction or deletion of data is carried out to according to agreed criteria and not according to personal preferences of individuals.

8. Records Destruction

8.1. The Helping Hands Retention Schedule defines the retention periods for all records and documents held by Helping Hands. Prior to destruction of any record, a review is carried out to determine whether it still needed or if it should be retained to fulfil a business purpose.

8.2. A record of the destruction activity must be kept as data subjects or supervisory authorities may require proof of the deletion of the relevant data.

8.3. The decision to retain records for longer than stated in the retention schedule needs to be justifiable and documented to avoid a breach of GDPR and the Data Protection Act 2018.

8.4. The review and destruction of paper and electronic procedures is covered in clauses 11.0 to 15.0.

8.5. Helping Hands systems and applications may also automatically archive, delete or purge data that has reached the end of the retention period.

8.6. Helping Hands systems and devices that are made redundant are decommissioned and archived so that historical data will no longer be accessible or available unless authorised by the TechTeam.

9. Data Cleansing & Minimisation

9.1. Personal data is collected and used for everyday business operations and whilst it is in use, it is best practice to regularly review and update personal data by correcting inaccurate information and data cleansing to comply with UK GDPR data minimisation and accuracy principles.

9.2. Processing personal data that is not relevant or needed results in unnecessary costs associated with storage and security, increases the risk of using such data in error and makes it more difficult to respond to subject access requests in a timely manner.

9.3. Personal data has to be archived for legal and documentation purposes, once the initial purpose for data collection and the lawful basis for processing has expired.

9.4. The lawful basis expiration typically occurs when a contract or service is terminated, the right to be forgotten is invoked or consent to use data by an individual is withdrawn.

9.5. Personal data or record at the end of the retention period must be reviewed, if stated, to determine whether it can be destroyed or deleted.

10. Right to be Forgotten

10.1. A flexible approach needs to be applied to requests for erasure also known as the 'right to be forgotten'. This policy can be used to consider early data deletion or destruction if appropriate.

10.2. Refer to the retention schedule as not every record or document can be deleted at the request of the data subject. The right to be forgotten is not absolute and only applies if:

10.2.1. The personal data is no longer necessary for the purpose which it was originally collected or processed for.

10.2.2. The lawful basis for processing or retaining data is consent, and the individual withdraws their consent.

10.2.3. Relying on legitimate interests as the lawful basis for processing and the individual objects to the processing of their data. Data must be deleted if there is no overriding legitimate interest to continue this processing.

10.2.4. Processing the personal data is for direct marketing purposes and the individual objects to processing.

10.2.5. Personal data has been processed unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle).

10.2.6. Complying with a legal obligation.

10.2.7. Processing personal data to offer information society services to a child.

11. Destruction Review Process and Authorisation

11.1. Reviews must be undertaken by employees in a managerial or senior position. This is to safeguard against the permanent loss of essential information as a result of malicious or unintentional destruction of data.

11.2. A review must be carried out for every record type to determine if retention is still necessary to fulfil a business need. The following considerations must be taken:

11.2.1. The retention period should be calculated from the end of the calendar or accounting year following the last entry on the record or termination date.

11.2.2. The actions set out in the retention schedule for each record type, Statutory or nonstandard retention period and additional notes should form the basis of the decision-making process.

11.2.3. Consider any involvement that could extend the retention such as complaints or appeals that were not resolved satisfactorily.

11.2.4. Consider precedent and historical nature of the record.

11.2.5. Consider any business requirements / instructions of significance such as historical, archival or risk of litigation.

11.2.6. Factor the value of such records to future generations that may not be fully anticipated at the present time

11.3. It is important to note that not all the above considerations will apply, so decisions need to be based on a common-sense approach and exercise ‘good judgement’.

11.4. A decision to extend retention must be documented and the reasons explained to justify this decision.

11.5. Decisions to extend retention should comply with the provisions of the UK GDPR, Data Protection principles and relevant Statutory Laws (e.g. financial records)

11.6. The decision to destroy or deletion must be authorised by a line manager or in the absence of one, escalated up the hierarchy to the next senior manager.

11.7. If there is no retention period in place for a record, the manager must consult with the Data Protection Officer (DPO), to assign an appropriate retention period and update the retention schedule. The decision to destroy or delete data will be authorised by the DPO.

12. Destruction of Paper Records

12.1. The destruction of paper records is an irreversible and permanent act.

12.2. Paper records that contain sensitive or confidential information must be disposed as confidential waste in the certified waste disposal bins provided. Alternatively, employees must use the approved GDPR – compliant machine cross-shredders available.

13. Deletion of Electronic Records

13.1. Data that is deleted will no longer be visible, accessible and cannot be recovered in accordance with data protection regulations, even if deletion was due to a malfunction or an error of the user triggering the deletion.

13.2. Deletion of electronic records is achieved by manually using the delete function on the system the data is stored on. This action transfers the data to a permanent archive in the electronic environment to be overwritten or destroyed.

13.3. Records due for deletion at the end of the retention period must include archived records.

13.4. Refer to the Helping Hands Data Map to know the location of the data and which systems exchange data with each other. This includes data stored on cloud services.

13.5. Data that cannot be deleted because it is stored on a shared system or on a database that contains additional records that still needs to be retained must be put ‘beyond use’ by contacting the TechTeam.

13.5.1. Beyond use may involve selective deletions, data encryption or anonymisation to render such data irretrievable until it can be permanently deleted.

13.6. Access Care Planner and Access People Planner requires data to be manually archived and / or anonymised as required.

13.7. Access Screening requires both archiving of background checks, which should then be followed by data purging (deletion) at the end of the retention period. Both are manual processes.

14. Data Anonymisation and Auto-Delete

14.1. The technical orchestration and complexity of data removal makes it difficult to automate all data removal, but Helping Hands uses several systems that do carry out data anonymisation or deletion as part of an automated process at the end of the agreed retention periods.

14.2. Automation reduces the amount of manual work needed, the risk of human error and retains an audit log of the deletion activity. Refer to available Data Maps to assist with data location.

14.3. Access Recruit

14.3.1. Access Recruit is set to data cleanse by archiving applications after 183 days from the date of completion. Once archived, specific details, identifiers and attached files can no longer be viewed.

14.3.2. Archived data is then auto deleted after 1200 (3yrs) and 400 days (1yr) for successful and unsuccessful applications respectively.

14.3.3. Incomplete applications are set to autodelete after 12 months if user account is inactive but can also be deleted manually at the candidate's request.

14.3.4. The profile and user account of a candidate is set to auto delete, after 12 months, from the date the portal account was activated unless the request to reactivate the account, sent prior to the deletion date, is accepted by the candidate.

14.3.5. Early deletion of candidate data, at the request of the candidate, is possible by manually overriding the system. This will permanently delete the profile, user account and all applications made by that candidate. This can only be actioned by the TechTeam.

14.4. Access CRM

14.4.1. Access CRM automatically deletes contact data after 6 months. CRM data that has been integrated with Access People Planner must be deleted manually as outlined in section 13.0

14.5. Access Care Planning

14.5.1. The retention of location data collected through the electronic monitoring apps such as Mobizio / Care Planning is automatically archived after 13 months and anonymised.

14.5.2. Reports containing location data that are generated and / or saved must be reviewed and manually deleted as required.

15. Evidence of Destruction

15.1. To evidence destruction of existing paper customer MAR and visit records held at the off-site archiving, a deletion log is maintained.

15.1.1. Additional notes referencing any records not deleted and an explanation to justify continued retention is documented.

15.1.2. This spreadsheet is kept in a secure location with limited access to the document via the GDPR Coordinator.

15.1.3. It must not be printed, copied or transmitted without appropriate security measures in place.

16. Helping Hands Retention Schedule

16.1. The Helping Hands Retention Schedule is located in this policy, Appendix One.

16.2. This schedule is reviewed periodically to reflect changes to legislation and to add new records when required.

16.3. It is the responsibility of Asset owners to ensure deletion of records as per the Retention Schedule and requirements outlined in points 11.0 to 15.0.

TRAINING

Is training required?	Yes
Details of training	Awareness from Compliance Coordinator GDPR Learning Management System - GDPR

COMPLIANCE

How is compliance with the Policy going to be monitored	• GDPR Steering Group • Quarterly Governance meetings for service review and improvement • Data Incident Notification (DIN) reporting • Complaints and Incident reporting • Document management and review process

EQUALITY IMPACT ASSESSMENT AND PROCEDURAL INFORMATION

	Positive / Negative / N/A	Comments
Does the document have a positive or negative impact on one group of people over another on the basis of their:		
• age?	NA	
• disability?	NA	
• gender reassignment?	NA	
• pregnancy and maternity (which includes breastfeeding)?	NA	
• race (including nationality, ethnic or national origins or colour)?	NA	
• marriage & civil partnership	NA	
• religion or belief?	NA	
• sex?	NA	
• sexual orientation?	NA	
If you have identified any potential impact (including any positive impact which may result in more favourable treatment for one particular group of people over another), are any exceptions valid, legal and/or justifiable?	NA	
If the impact on one of the above groups is likely to be negative:		
• Can the impact be avoided?	NA	
• What alternatives are there to achieving the document's aim without the impact?	NA	
• Can the impact be reduced by taking different action?	NA	
• Is there an impact on staff, client or someone else's privacy?	NA	*If yes, privacy impact assessment required*

What was the previous version number of this document?	Version 01	
Changes since previous version	Amended Retention Schedule for: • Adult care records • Adult safeguarding records • Personnel records pertaining to safeguarding allegations	
Who was involved in developing/reviewing /amending the Policy?	GDPR Coordinator Quality Development Lead	
How confidential is this document?	Restricted	Can be shared freely within Helping Hands but NOT outside

References	*References are the evidence base for the document (legislation, codes of practice etc., and need to be current)*
Associated Documents	*Appendix One – Retention Schedule* *Information Governance Policy* *Data Protection Policy*

Appendix One – Retention Schedule

RECORD TYPE	RECORD SUB-TYPE	RETENTION START	RETENTION PERIOD	ACTION AT END OF RETENTION PERIOD	NOTES
Care Records	Adult Care Records (paper)	End of care or customer last seen	8 years	Review and if no longer needed, destroy	Check for any involvement that could extend the retention. E.g. requests, complaints, appeals etc
	Adult Care Records – Safeguarding (digital)	End of care or customer last seen	8 years	Review and if no longer needed, destroy	
	Adult Care Records (digital)	End of care or customer last seen	8 years	Review and if no longer needed, destroy	
	Access Electronic Care Records	End of care or customer last seen	8 years	Review and if no longer needed, destroy	
	Electronic call monitoring/ care planning app data	Creation	End of contract. Revised to 13 months from March 2021	Archived by software provider or manual deletion/ anonymisation	Assistance from IT support to delete or anonymise data
	Feedback data, reviews and social media content (including images)	Creation	See notes	See notes	See Marketing/ Design section of this schedule
Telephony Systems	Telephony Systems (record of call log)	Creation	Duration of service provider contract		.
	Telephone recordings	Creation	10 months	Auto - deletion	Telecom provider has agreed protocols in

					place to retain/delete outside of this period subject to the required access privileges
Corporate Governance	Article of Incorporation	Creation	Permanent		
	Annual corporate filings	Creation	Permanent		
	Board policies and meeting minutes	Creation	Permanent	Transfer to a place of deposit	
	Chief Executive records	Creation	Up to 20 years or Permanently for historical purposes	Transfer to a place of deposit	May include emails and correspondence if not already included in board papers and if considered to be of archival interest.
	Committees/ Groups/Sub committees	Creation	6 years	Review and if no longer needed, destroy	Includes projects and departmental business meetings.
	Accident books, accident record/report	From the date of the last entry (or, if the accident involves a child/young adult, then until that person reaches the age of 21)	3 years		Statutory period under The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances.
	Serious Incidents, events or occurrences	Date of incident	20 years	Review and consider transfer to a place of deposit	The Public Records Act 1958 limits retention of records to 20 years and must either be transferred to a place of deposit or destroyed 20 years after record has been closed.
	Minor Incidents	Date of incident	10 years	Review and if no longer needed, destroy	

	Assessments under health and safety regulations and records of consultations with safety representative and committees	Creation	Permanently		
	Non-Clinical compliance records	End of year to which the report relates to	12 years	Review and if no longer needed, destroy	
	Policies, strategies and operating procedures including business plans	Live document	Policies First and second review	Review and consider transfer to a place of deposit	Archived copies kept for the life of the business + 6 years
Communications	Intranet site	Creation	6 years	Review and consider transfer to a place of deposit	
	Active Email inboxes and shared inboxes	Release date	2 years for all users and 7 years for director and senior leadership team		Review and if no longer needed, delete emails in line with GDPR storage limitations and best practice
	Active Email sub folders (including sent and deleted items)	Release date	2 years for all users and 7 years for director and senior leadership team		
	Email Calendar items, appointments, meetings and all attachments	Release date	13 months		
	Email accounts	When disabled/ deactivated	3 months		This period can be extended if litigation hold is enabled. Emails following deactivation

					of account is irretrievable.
	Website	Creation	6 years	Review and consider transfer to a place of deposit	
	Live Chat transcripts / history	Creation	1 year		
Employee Records	Duty Roster	Close of financial year	6 years	Review and if no longer needed, destroy	
	Personnel file (employees) including disciplinary records	End of employment	6 years (if summary is created)		Includes but not limited to evidence of right to work, security or criminal checks. Information on Access self-serve can be amended/deleted by employee at any time
	Personnel file (employees) pertaining to safeguarding allegations	End of employment	8 years	Review and if no longer needed, destroy	Does not include in relation to malicious allegations
	Personnel record summary	6 years after end of employment	75th birthday	Place of deposit for continued retention or destroy	
	Recruitment records	End of employment	6 years	Review and if no longer needed, destroy	Merged candidate data includes successful applications and interview notes
	Parental and annual leave records	End of employment	6 years	Review and if no longer needed, destroy	
	Redundancy details, calculations of payments, refunds, notification to the Secretary of State	From date of redundancy	6 years	Review as per legal requirement	

	Training and performance records	Creation	6 years	Review and if no longer needed, destroy	Statutory and mandatory training records to be kept for 10 years after training completion
	Exit interview notes/ feedback	End of employment	12 months	Review and if no longer needed, destroy	
	Electronic call monitoring/ location data	Creation	End of contract. Revised to 13 months from March 2021	Archived by software provider or manual deletion/ anonymisation	Assistance from IT support to delete or anonymise data
	Employee profiles	Creation	End of employment	Delete/destroy by shredding	Archive or destroy profiles no longer in use
	Employee Badges	Creation	End of employment	Destroy to render it unusable	
Recruitment	Successful Applications	Completion date of application	3 years	Review in line with recruitment and selection policy	Retention extended in line with employee records
	Unsuccessful Applications	Completion date of application	6 months	Review in line with recruitment and selection policy	Destroy in line with deletion process and work instruction
	Incomplete applications	Creation	12 months	Review ATS account and if no longer active, delete	Auto delete set to 12 months unless request to reactivate account is accepted
	Contact Data - successful candidates	Creation	End of employment	Review and if no longer needed, destroy	Retention extended if processing is still required under legitimate interest
	Contact data - potential candidates	Creation	6 - 12 months	Review and if no longer needed, destroy	Retention relates to contact information for marketing purposes. Candidate can also delete ATS account at any time.
	Contact data - unsuccessful candidates	Creation	12 months	Review and if no longer	Data may be anonymised and used for statistical

				needed, destroy	/analytical purposes only
Sales	CRM data	End of contract	3 years	Review and destroy if no longer needed or at the request of the person if no longer active.	Data must be anonymised if used for statistical /analytical purposes
	Contact data – Facebook Messenger Twitter	Creation	n/a	Destroy when no longer needed to facilitate information management	Data kept only for it is needed to respond to enquiry or refer to Customer support teams
Marketing/ Design Team	Distribution lists/spreadsheets	Creation	n/a	Kept until person unsubscribes or requests to be removed	Regular data cleansing and delete if no longer in use
	Platform data comments, online reviews, profile pictures	Creation	n/a	Kept until person requests to be removed	Reasonable attempts must be made to delete historical content where possible
	Customer survey feedback data	Creation	6 - 12 months	Review and if no longer needed, destroy	Data may be anonymised and used for statistical /analytical purposes only
	Employee survey feedback data	Creation	3 years	Review and if no longer needed, destroy	Data may be anonymised and used for statistical /analytical purposes only
	Customer reviews	Creation	n/a	Review and destroy if no longer needed or consent is withdrawn	Data may be anonymised and used for statistical /analytical purposes only
	Employee reviews	Creation	n/a	Review and destroy if no longer needed or	Data may be anonymised and used for statistical /analytical purposes only

				consent is withdrawn	
	GDPR consent forms	Creation	3 years or end of contract	Review every 3 year or until consent is withdrawn	
	Employee or customer image/profile	Creation	n/a	Review and destroy if no longer needed or consent is withdrawn	Refer to relevant GDPR consent form in review process
Procurement / Property	Supplier Contracts	End of contract	6 years	Review and if no longer needed, destroy	
	Amendments to contracts - changes, variations and extensions	End of contract	6 years	Review and if no longer needed, destroy	
	Tenders (successful)	From award of contract	6 years	Review and if no longer needed, destroy	
	Tenders (unsuccessful)	After date of last paper	1 year	Review and if no longer needed, destroy	
	Disputes over payment	End of contract	6 years		
	CCTV	Creation	180 days	Review and if no longer needed, data overwritten or destroyed	Length of retention is determined by purpose e.g. crime prevention. See CCTV Policy
	Leases	Termination of lease	12 years	Review and if no longer needed, destroy	
	Photographic collection of service locations/events/activities	Close of collection	No more than 20 years	Consider transfer to a place of deposit	Retain if for historical legacy of running and operation of business or use for legal enquiries
Finance	Fiscal policies and procedures	Creation	Permanent		
	Financial statements	Creation	Permanent		

	Permanent audits	Creation	Permanent		
	General Ledger	Creation	Permanent		
	Accounts	Close of financial year	3 years	Review and if no longer needed, destroy	Statutory period under Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
	Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred with the board papers	Transfer as soon as practically possible
	Debtor records (cleared)		2 years	Review and if no longer needed, destroy	
	Debtor records (uncleared)		6 years	Review and if no longer needed, destroy	
	Financial records of transactions	End of financial year	6 years	Review and if no longer needed, destroy	
	Income tax and NI returns, income tax records and correspondence with HMRC	After the end of the financial year to which they relate	Not less than 3 years		Statutory period under The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended,
	Expenses	Close of financial year	6 years after audit	Review and if no longer needed, destroy	
	Purchase order books/records	Creation	6 years		
	Petty cash	End of financial year	2 years	Review and if no longer needed, destroy	
	Payroll records (also overtime and bonuses)	Close of financial year	6 years	Review and if no longer needed, destroy	Statutory period under Taxes Management Act 1970

	National minimum wage records	End of the pay reference period following the one that the records cover	3 years		Statutory period under National Minimum Wage Act 1998
	Records relating to working time	From date of creation	2 years		Statutory period under The Working Time Regulations 1998 (SI 1998/1833)
	Timesheets (original records)	Creation	2 years after audit	Review and if no longer needed, destroy	
	Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	End of the tax year in which the maternity period ends	3 years		Statutory period under The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
	Statutory Sick Pay records, calculations, certificates, self-certificates	End of period of sick leave	3 months (see notes)		Keep sickness records to best suit their business needs. It is advisable to keep records for at least 3 months after the end of the period of sick leave in case of a disability discrimination claim. However, if there were to be a contractual claim for breach of an employment contract it may be safer to keep records for 6 years after the employment ceases.
	Retirement Benefits Schemes - records of notifiable events, for example, relating to incapacity	End of the scheme year in which the event took place	6 years		Statutory period under The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

	Pension scheme investment policies including Pensioner's records	From the end of any benefit payable under the policy	12 years		
Legal / Complaints / Information Rights	Complaints case file	Closure of incident (see notes)	10 years	Review and if no longer needed, destroy	An incident is not closed until all subsequent processes have ceased including litigation. The record must not be kept on the individual's file but maintained separately.
	Fraud case files	Case closure	6 years	Review and if no longer needed, destroy	
	Tribunal case records	Close of financial year	10 years		These records should form a distinct separate record held by the manager or payroll team for processing
	Litigation records	Closure of case	10 years	Review and consider transfer to a place of deposit	
	Trademarks/copyrights/ Intellectual property	End of termination of licence/action	6 years after termination	Review and consider transfer to a place of deposit	
	Software licences	End of lifetime of software	Lifetime of software	Review and if no longer needed, destroy	
	SAR and disclosure correspondence	Closure of SAR	3 years	Review and if no longer needed, destroy	
	SAR (subsequent appeal)	Closure of appeal	6 years	Review and if no longer needed, destroy	