SA/16 - Data Protection Policy

PN:01

"Our policies embed our culture, establish boundaries and outline our expectations. They have been agreed by our Board(s) as best practice documents for the Group's decision making."

Policy Statement

Every day as a Group we will receive, use and store personal information about our customers, stakeholders and employees. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation.

We take our data protection duties seriously because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

This policy applies to all ateb Group Limited's, Mill Bay Homes' and West Wales Care & Repair's customers, stakeholders and employees.

Approval Date	Lead Contact	Review Date
27th January 2022	Data Protection Officer	November 2023

Policy Contents

2. Principles

The purpose of this policy and any other documents referred to in it, is to set out how ateb Group Limited, Mill Bay Homes and West Wales Care & Repair handles the personal data of our customers, stakeholders and employees. The policy details the basis upon which we will process any personal data we collect and process in line with the requirements of the Data Protection Act 2018 (**DPA**) and the retained EU law version of the General Data Protection Regulation (**UK GDPR**) (collectively referred to as the '**Data Protection Requirements**').

When we talk about **Personal Data** we mean data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Certain types of personal data are classed as **Sensitive Personal Data** (this is also sometimes described as "special category data"). This includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, such as with the explicit consent of the individual.

When we talk about **Processing**, we mean any activity that involves use of personal data. Processing includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

As a Group when processing personal data we comply with the **Data Protection Principles** that personal data will be:

a. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

b. collected only for specified, explicit and legitimate purposes (Purpose Limitation);

c. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

d. accurate and where necessary kept up to date (Accuracy);

e. not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

f. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

g. not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

h. made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

1. Lawfulness, Fairness and Transparency

We will only process personal data where it is required for a lawful purpose. The lawful purposes include: the individual has given their consent; the processing is necessary for performing a contract with the individual; for compliance with a legal obligation; to protect the data subject's vital interests; or for the legitimate interests of the business. When sensitive personal data is being processed, additional conditions must be met (see our Privacy Notices for further information).

When we rely on a data subject's consent, which will be in limited circumstances, we ensure that consent is indicated clearly, either by a statement or positive action, such as ticking a box. We respect a data subject's right to withdraw consent at any time and will record and honour any request. If a data subject asks to withdraw their consent but we consider that it is still necessary for us to continue to process their data and we have another lawful basis to do so other than consent, we will explain this to the data subject when their request is made.

2. Purpose Limitation

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. If we collect personal data directly from an individual, we will inform them of the following (if applicable) through our Privacy Notices and this policy:

a. the purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
b. where we rely upon the legitimate interests of the business to process personal data, what are the legitimate interests that are pursued.
c. the types of third parties, if any, with which we will share or disclose that personal data.
d. the fact that the Group intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place.
e. how individuals can limit our use and disclosure of their personal data.
f. information about the period that their information will be stored or the criteria used to determine that period.
g. their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
h. their right to object to processing and their right to data portability.
i. their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
j. the right to lodge a complaint with the Information Commissioner's Office (ICO).
k. other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
l. whether the provision of the personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract as well as whether the individual is obliged to provide their personal data and any consequences of failure to provide the data.
m. the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences or such processing for the individual.

The following Privacy Notices detail how we will process your data:

- Privacy Notice - Job Applicants
- Privacy Notice - Employees
- Privacy Notice - Customers
- Privacy Notice - Contractors/Suppliers
  Privacy Notice for Mill Bay Homes
- Privacy Notice for West Wales Care & Repair
- Cookie Policy

As our services improve, the above Privacy Notices may be updated.

3. Data Minimisation

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject. We ensure that excessive data is not collected and will not make unnecessary copies.

Employees must only process personal data when performing their job role requires it, and must not process personal data for any reason unrelated to their job duties.

This applies regardless of whether an employee is working at home, on site or in one of the Group's offices.

When data is no longer needed, we ensure that it is deleted, securely destroyed or anonymised in accordance with our retention guidelines which can be found at appendix 1 to this policy.

4. Accuracy

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date data.

We respect our customers/stakeholders/employees' rights to check the accuracy of any personal data we hold and request any amendments of the same.

5. Storage Limitation

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy or erase from our systems all data which is no longer required. Please see our retention guidelines at appendix 1 for more details.

6. Security, Integrity and Confidentiality

We will take appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed.

We will put in place policies, processes and technologies to maintain the security of all personal data from the point of determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with our policies or processes, or if they have/put in place adequate measures themselves.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. confidentiality means that only people who are authorised to use the data can access it.
b. integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
c. availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data will only be stored on central systems and not on personal devices.

We will ensure that our data security and confidentiality measures are not adversely affected where employees work from home, on site or in a hybrid manner.

We apply the following security measures:

a. Door Entry Controls: Any stranger seen in an entry-controlled area who is not wearing an ateb Group visitor badge is to be reported to the first available manager who will take necessary steps to identify that stranger.
b. use of strong passwords for electronic devices
c. secure lockable desks and cupboards. Desks and cupboards are to be kept locked if they contain confidential information of any kind. (Personal data is always considered confidential.)
d. Homeworking: protocols for the security of data where employees work from home, including: ensuring that employees have a password-protected VPN where they use a shared computer and that passwords are not shared with members of their households; asking employees to be aware of visitors in their home who can overlook their workspaces; asking employees not to take hard copies of documents home, and/or to keep documents secure and return them to the workplace as soon as possible if it is necessary to take documents home on occasion and if documents are no longer needed returning them to the workplace and disposing of them confidently using the confidential waste facilities in place at the office; asking employees to keep their homeworking spaces secure and not to leave company equipment or documents in unlocked premises or in vehicles; and notify the Governance and ICT Teams if their work device is lost/stolen.
e. Data Minimisation: Only collecting sufficient personal data for the specified purposes.
f. Pseudonymisation and encryption of data where possible. Replacing any identifying characteristics of data with a pseudonym, in other words a value which does not allow the data subject to be directly identified.
g. ensuring that all personal data sent outside of the Group via electronic means is encrypted with security measures, e.g., password protected.
h. Methods of Disposal: Paper documents are to be shredded or placed in confidential waste bags to be collected by an approved confidential waste carrier and disposed of securely. Digital storage devices are to be physically destroyed when they are no longer required.
i. Equipment: Employees are to ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC, laptop or tablet, or ensure a password protected screensaver is activated as soon as possible when their equipment is left unattended. All phones, iPads and tablets issued by the Group are to be encrypted/password protected, depending on the device. Employees using their own devices for work purposes need to ensure they use 2 factor verification for emails and MS Teams and are not to save any customer personal data on their systems.
j. not transferring data to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

Employees must comply with all of the above measures at all times, and must not attempt to circumvent any of the administrative, physical or technical safeguards we

implement and maintain in accordance with the Data Protection Requirements. This applies regardless of whether the employee is working in the office, on site or at home. For example, an employee who has a hard copy document stored at home must return it to the office for secure destruction in accordance with paragraph d. above.

Employees must read the above in conjunction with our guidance on IT Security Measures which further details the security measures in place on electronic devices supplied to employees.

7. Transfer Limitation

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

We do not normally transfer data outside of the UK.

Employees may only transfer personal data outside of the UK if one of the following applies:

a. the UK has issued regulations confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subject's rights and freedoms;

b. appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism;

c. the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

d. the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

8. Data Subject's Rights and Requests

We will process all personal data in line with our customers'/stakeholders'/ employees' rights in particular their right to:

a. confirmation as to whether or not personal data concerning them is being processed.
b. request access to any data held about them by a data controller.
c. request rectification, erasure or restriction on processing of their personal data.

d. lodge a complaint with a supervisory authority.
e. data portability.
f. object to processing, including for direct marketing.
g. not be subject to automated decision making, including profiling in certain circumstances.
h. not have their personal data transferred to people or organisations situated in countries without adequate protection and us without first having advised the individual.
i. be notified of a personal data breach if it is likely to result in a high risk to their rights and freedoms.

A customer/stakeholder/employee wanting to invoke any rights listed above or wanting to make a Subject Access Request (SAR) (request to access personal data), is to make a formal request in writing to the Data Protection Officer.
We will verify the identity of any individual requesting data under any of the rights listed above, for example by requesting photographic ID or speaking to them in person.

Direct Marketing

We obtain our data subjects' prior consent for electronic direct marketing (for example by email, text or automated calls.) The limited exception for our existing customers known as 'soft opt in' allows us to send marketing texts or emails if we have obtained contact details in the course of providing a commercial service to our customers and we are marketing similar products or services and we gave our customers the opportunity to opt out of this when first collecting their details and do so in every message thereafter.

We give our customers the right to object to direct marketing in an intelligible manner and any objections are honoured, recorded and respected. If a customer opts out at any time, their details should be supressed (meaning retaining just enough information to ensure that marketing preferences are respected in the future) as soon as possible.

Data Protection Impact Assessments (DPIAs)

A DPIA must be conducted if we carry out any "high-risk processing activities", such as processing of data of a highly personal nature, or large-scale processing of data; or any major project which involves the use of personal data.

A DPIA must:

a. Describe the nature, scope, context and purpose of the processing activity;
b. Assess necessity, proportionality and compliance measures;
c. Identify and assess any risks posed to individuals; and
d. Identify any additional measures needed to mitigate those risks.

Employees must consult with the DPO if they think that a DPIA may be necessary.

3. Responsibilities

Group

This is a Group Policy which applies to all companies within the Group structure.

Board of Management

The ateb Board of Management, as the parent company within the Group, is responsible for approving the use of this policy.

All subsidiary Boards are responsible for ensuring this policy is being used within their respective companies.

All Line Managers

All line managers are responsible for ensuring that this policy operates effectively within their team which includes the following duties:

- Ensuring their team members understand their responsibilities under this policy
- Ensuring their team members attend training opportunities which include new starter training and refresher training. If any team members require additional training, line managers are to inform the DPO.
- Keeping records of customer consents and withdrawals of consents and sharing the same with the Governance team to include in a central record.
- Ensuring that processes under their control comply with the Data Protection Requirements and principles listed above and protect the processing of personal data.
- Reporting any Subject Access Requests or third party requests and any data protection breaches to the DPO and Governance team as soon as possible
- Informing the DPO of any changes required to the Customer Privacy Notices if a change in their service area leads to a change in the way they process customer personal data.
- Carrying out Data Protection Impact Assessments before the commencement of a project if their work involves implementing major system or business change programmes involving the use of personal data including:
  a. use of new technologies or changing technologies (programmes, systems or processes)
  b. automated processing including profiling
  c. large scale processing of sensitive data
  d. large scale systematic monitoring of a publicly accessible area (CCTV)
- Putting in place adequate Information Sharing Protocols with partners such as statutory bodies when working collaboratively and are required by law to share information with partners (WASPI agreements).
- Ensuring partners or contractors/consultants engaged to provide a service either comply with or have their own data protection policy which meets the

Data Protection Requirements. All contracts should include data protection clauses.

Line managers are to seek the advice of the DPO if they are unsure about how their service area is meeting the Data Protection Principles listed in section 2 of this policy to include direct marketing, or if they need any advice regarding their responsibilities under this policy.

All Employees

All employees are responsible for ensuring they understand this policy and for complying with this policy when processing a customer's personal data and engaging in marketing activities.

Employees' responsibilities under this policy include the following:

- Attending data protection training made available to them and for informing their managers if they have not been offered the same.
- Complying with our Information Security Measures policy and ICT Equipment Usage policy.
- Reporting all data breaches to the DPO and Governance Team as soon as they become aware of a suspected breach so that they can be supported in dealing with the same. There is a duty on the DPO to report reportable breaches to the ICO within 72 hours, so the DPO needs to be aware of any breaches.
- Preserving all evidence relating to a potential breach so that it can be investigated and rectified.
- Reporting any requests by customers to access their data (Subject Access Requests) to the DPO or Governance team so requests can be recorded and dealt with within a reasonable timeframe (no longer than a month).
- Recording and reporting to the DPO or Governance Team any request by customers to implement any of their rights listed in section 2 of this policy.
- Reporting any third party requests for data to the DPO or Governance team for advice as to whether the same can be disclosed.
- Refraining from accessing, disclosing, or processing any personal data other than is necessary to carry out their employee duties.
- Obtaining consent before taking and using photographs of customers/ employees or stakeholders.
- Keeping and maintaining accurate records of any data processing activities carried out in the course of their jobs, including records of data subjects' consents and procedures for obtaining consents.

Stakeholders

All partners, contractors and consultants engaged with the Group are required to comply with this Data Protection policy when processing Group customer data or evidence to the Group how their own policies meet the Data Protection Requirements.

Customers

Customers are responsible for informing the DPO should they have any concerns about the way the Group is using their data. If customers are not satisfied with the response from the DPO they have the right to report a complaint to the Information Commissioner's Office:

ICO Wales
2nd Floor, Churchill House
Churchill Way
Cardiff
CF10 2HH

Customers are asked to inform the Group if their contact details change so we can keep their details accurate.

When making a request to access personal data (Subject Access Request) or when accessing any rights outlined in section 2 of this policy, customers need to put their request in writing for the attention of the DPO. We will aim to record and action any request within 30 days of receipt. We will require identification from customers before providing any personal data.

Key Operational Role Responsibilities

In addition to the responsibilities listed above, the following key role(s) have specific responsibilities for the operational delivery of the policy across the Group:

Data Protection Officer (DPO)

The DPO is responsible for ensuring that there are adequate learning, development, guidance and support opportunities to implement this policy. This includes ensuring there is training available for new starters and annual refresher training for employees.

Any questions about the operation of this policy or the data protection requirements should be directed to the DPO.

Details of the DPO:

Ceri Morgan
ateb Group Limited
Meyler House
St Thomas Green
Havefordwest SA61 1QP

4. Control

The DPO is the lead contact for this policy and for ensuring it remains operationally effective. The DPO will review this policy at least every 2 years.

This policy is a dynamic document and will be amended as required following service reviews or changes to the operating environment.

Board approval will be obtained before any amendments are published and employees will receive refresher training as applicable.

5. Links to other documents

Internal

- Privacy notices for Customers, Employees, Job Applicants and Partners can be found on our website ateb Privacy Notices or Mill Bay Homes Privacy Notice or WWC&R Privacy Notice
- Data Processing Schedule www.atebgroup.co.uk
- Cookies Policy
- Employee Data Protection Procedure
- CCTV Policy
- Guidance on IT Security Measures
- Guidance on Computer Usage, BYOD, data breaches, SAR, third party requests can be found on Yammer or requested from the Governance team.

External

- Data Protection Act 2018/ General Data Protection Regulation
- Information Commissioner's Office ICO Wales

ateb Policy Number: PN01

SA/16 – Data Protection Policy

Additional help

Contact our Governance team quoting the policy reference: PN01

Tel: **01437 763688**
Email: **hello@atebgroup.co.uk**
Facebook **@atebgroup**
Face to Face: **Meyler House, Haverfordwest, SA61 1QP**

Version History

Ver	Date	Changes
1	Nov 2019	Policy approved by Board
2	Jan 2022	Policy reviewed and approved by Board
3		

DATA RETENTION SCHEDULE

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
1. Governance								
1.1	Governance	Organisation wide Corporate Plans, Policies, Business Continuity, Risk Management and Strategies	Superseded document	N/A	1 year after superseded (longer if required for historical reasons)	Securely Destroy		Best practice
1.2	Governance	Governance documentation		N/A	Life of company	Securely Destroy		Required for charitable status.
1.3	Governance	Constitution, Aims and Objectives		Life of company	Life of company	Securely Destroy		Required for charitable status.
1.4	Governance	Record of HMRC confirmation of charitable status	End of financial year	Minimum 1 year to end of financial year - required for Annual Return as a minimum	Life of company	Securely Destroy	ICSA	Annual return and best practice.
1.5	Governance	Record of charitable registration		Life of company	Life of company	Securely Destroy	ICSA	Best practice.
1.6	Governance	Certificate of Incorporation		Life of company	Life of company	Securely Destroy	Companies Act 2006 section 15	Legal compliance
1.7	Governance	Memorandum of Association		Life of company	Life of company	Securely Destroy	Companies Act 2006 section 32	Legal compliance
1.8	Governance	Articles of Association/ Model Rules		Life of company	Life of company	Securely Destroy	Companies Act 2006 section 32	Legal compliance
1.9	Governance	Certificate of registration with housing regulator		Life of company	Life of company	Securely Destroy	ICSA	Best practice
1.10	Governance	Record of registration and certificate of incorporation for change of name		Life of company	Life of company	Securely Destroy	Companies Act 2006 section 80	Legal compliance
1.11	Governance	Registration documentation (Co-operative and Community Benefit Societies)		Life of company	Life of company	Securely Destroy	Co-operative and Community Benefit Societies Act 2014 section 3	Legal compliance
1.12	Governance	Internal Audit correspondence, terms of reference, meeting minutes, related papers and reports	After audit	N/A	5 years	Securely Destroy		Best practice
1.13	Governance	Board member documents – apt letters, SLAs, bank details etc.	Membership ceases	6 years after board membership ceases though some details should be destroyed when membership ceases e.g. bank details etc.	6 years	Securely Destroy	GDPR Article 5(1) (e) requires that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary CA 2006 recommendation for docs post termination of directorship	Legal compliance
2. Data Governance								
2.1	Data Governance	Emails	No longer active	receipt of email	Archived after 6 months Destroyed after 2 years	Securely Destroy	Ofcom National archive guidance ranges from 90 days to four years.	Best practice
2.2	Data Governance	CCTV	Date of recording	Minimum time necessary	30 days	Securely Destroy	DPA	Best practice
2.3	Data Governance	Call Recordings	Date of recording	Minimum time necessary	6 months	Securely Destroy	FCA Handbook, conduct of business 11.8	Best practice
2.4	Data Governance	Data Subject Access Requests	Data sent	6 months	1 year	Securely Destroy	ICo	Best practice
2.5	Data Governance	Films / Videos	Date of recording	Minimum time necessary	3 years	Securely Destroy		Best practice
2.6	Data Governance	Data Breach Records	Date of recording	N/A	6 years	Securely Destroy		Best practice
2.7	Data Governance	Fraud Records	Date of recording	6 years	6 years	Securely Destroy	FCA Handbook	Best practice
2.8	Data Governance	Data Subject Access Requests	Data sent	6 months	1 year	Securely Destroy	ICO	Best practice
3. Meetings								
3.1	Meetings	Notice of meetings		N/A	6 years	Securely Destroy		In case of challenge to validity of meeting or resolutions
3.2	Meetings	Executive meeting agendas, papers, minutes and resolutions		N/A	10 years	Securely Destroy		Best practice

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
3.3	Meetings	Board and Committee meeting minutes and resolutions	Date of meeting	10 years from the date of the meeting of extant company or life of company	10 years from the date of the meeting of extant company or life of company	Securely Destroy	Companies Act 2006 section 248 and 249	Legal compliance
3.4	Meetings	Board and Committee meeting agendas and papers	Date of meeting	10 years from the date of the meeting of extant company or life of company	10 years from the date of the meeting of extant company or life of company	Securely Destroy	Companies Act 2006 section 248 and 250	Best practice (if required to support minutes and resolutions)
3.5	Meetings	Shareholder meeting minutes and resolutions	Date of meeting	Life of company	Life of company	Securely Destroy	Companies Act 2006 section 356	Legal compliance
3.6	Meetings	Shareholder meeting agendas and papers	Date of meeting	N/A	Life of company	Securely Destroy		Best practice (if required to support minutes and resolutions)
3.7	Meetings	Minutes and resolutions of trustees (charities)	Date of meeting	Life of company	Life of company	Securely Destroy	Charity Commission requirement CC48	Legal compliance
4. Regulations and Statutory Returns								
4.1	Regulations and Statutory Returns	Audited financial statements	Submission	Minimum of 3 years	6 years	Securely Destroy	Companies Act 2006 section 388 and Professional Standards Authority and National Archives recommendations for best practice	Legal compliance and best practice
4.2	Regulations and Statutory Returns	Sealing register		Life of company	Life of company	Securely Destroy	Companies Act 1985	Legal compliance
4.3	Regulations and Statutory Returns	Annual Statutory Returns to the Regulator	Submission	Minimum of 1 year from submission	Life of company	Securely Destroy	Co-operative and Community Benefit Societies Act 2014 section 90	Legal compliance and best practice
4.4	Regulations and Statutory Returns	Register of directors and secretaries		Life of company	Life of company	Securely Destroy	Companies Act 2006 section 162	Legal compliance
4.5	Regulations and Statutory Returns	Register of shareholding members		Life of company	Life of company	Securely Destroy	Companies Act 2006 section 113	Legal compliance
4.6	Regulations and Statutory Returns	Register of share certificates		Life of company	Life of company	Securely Destroy	Companies Act 1984 s.325	Legal compliance
4.7	Regulations and Statutory Returns	Declarations of interest		Life of company	Life of company	Securely Destroy	Company Act 2006 section 177 (implied)	Legal compliance
4.8	Regulations and Statutory Returns	List of members (Communities & Benefit Society')		Life of company	Life of company	Securely Destroy	Registrar of Friendly Societies	Required by Registrar of Friendly Societies
4.9	Regulations and Statutory Returns	Nursing home and residential care homes registration certificates	End of management	N/A	7 years following end of management	Securely Destroy	Care Quality Commission Guidelines	Best practice
4.10	Regulations and Statutory Returns	Nursing home and residential care homes inspection reports	End of management	7 years following end of management	7 years following end of management	Securely Destroy	Care Quality Commission Guidelines and Limitation Act 1980	Legal compliance and best practice
5. Strategic Management								
5.1	Strategic	Business Plans and supporting documentation	End of Business Plan Period	N/A	5 years	Securely Destroy		Best practice

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
6. Insurance								
6.1	Insurance	Current/former policies: - crime cover - engineering inspection - motor insurance - property damage - loss of commercial rent - housing contents - office contents - works in progress cover - business interruption cover - all risks cover - engineering insurance - personal accident for staff - professional indemnity - crime/fidelity cover	End of policy term	Life of company	Life of company	Review	Limitation can commence from knowledge of potential claim and not necessarily the cause of the claim. N.B. Housing Association Boards must annually reaffirm formally their continuation of the Voluntary Board Members Liability Policy (automatically provided via NHF membership). NCVO (National Council for Voluntary Organisations) recommends 3 years after lapse.	Legal compliance and best practice
6.2	Insurance	Certificate of Employers' Liability Insurance	End of policy term	N/A	40 years	Offer to Archives	2008 regulations removed requirement to retain for 40 years but need to be mindful of 'long tail' industrial disease claims, etc.	Best practice
6.3	Insurance	Annual Insurance schedule	End of year	N/A	Life of company	Securely Destroy	As current and former policies are kept permanently (above), schedules should be too. Best practice	Best practice
6.4	Insurance	Claims and related correspondence	End of settlement	N/A	2 years	Securely Destroy	Zurich Municipal recommendation. NCVO recommends 3 years after settlement	Best practice
6.5	Insurance	Indemnities and guarantees	End of policy term	N/A	6 years after expiry	Securely Destroy	Limitations Act 1980, Limitation for legal proceedings. 12 years if related to land.	Legal compliance
6.6	Insurance	Group health policies	End of benefits	N/A	12 years after cessation of benefit	Securely Destroy		Best practice
7. Finance								
7.1	Finance	Accounting records for Limited Company		6 years	6 years	Securely Destroy	Companies Act Section 388 recommends 3 years. Taxes Management Act 1970 (TMA) Sec20 (Taxes Management Act 1970) may require any documents relating to tax over 6 (plus) years	Legal compliance
7.2	Finance	Accounting records for Communities & Benefit Society' Society or Charity		N/A	6 years	Securely Destroy		Best practice
7.3	Finance - Cheques and associated records	Cash books/sheets	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.4	Finance - Cheques and associated records	Petty cash records/books/sheets Postage/courier account/cash records Register of postage expenditure Postage paid record Postage books sheets	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.5	Finance - Cheques and associated records	Creditors' history records	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.6	Finance - Cheques and associated records	Statements of accounts outstanding orders	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.7	Finance - Cheques and associated records	Vouchers – claims for payment, purchase orders, requisition for goods and services, accounts payable, invoices and so on	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
7.8	Finance - Cheques and associated records	Wages/salaries vouchers	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.9	Finance - Cheques and associated records	General and subsidiary ledgers produced for the purposes of preparing certified financial statements or published information	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.10	Finance - Expenditure records	Cash books/sheets	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.11	Finance - Expenditure records	Other ledgers (such as contracts, costs, purchases)	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.12	Finance - Expenditure records	Journals – prime records for the raising of charges	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.13	Finance - Expenditure records	Journals – routine adjustments	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.14	Finance - Expenditure records	Trial balances - Year-end balances, reconciliations and variations to support ledger balances and published accounts	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.15	Finance - Receipts and revenue records	Receipt books/butts Office copies of receipts – cashiers', cash register, fines and costs, sale of publications, general receipt books/butts/ records	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.16	Finance - Receipts and revenue records	Postal remittance books/records	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.17	Finance - Receipts and revenue records	Receipt books/records for imposts (such as stamp duty, VAT receipt books)	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.18	Finance - Receipts and revenue records	Cash registers - Copies of forms, Reconciliation sheets	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.19	Finance - Receipts and revenue records	Audit rolls, Summaries/analysis records	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.20	Finance - Receipts and revenue records	Debtors' records and invoices - debit notes rendered on debtors (such as invoices paid/unpaid, registers of invoices, debtors ledgers)	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.21	Finance - Receipts and revenue records	Debits and refunds - Records relating to unrecoverable revenue, debts and overpayments (such as register of debts written off, register of refunds)	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.22	Finance- Salaries and related records	Employee pay histories Note that the last three years' records must be kept for leavers, in either the personnel or finance records system, for the calculation of pension entitlement	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.23	Finance- Salaries and related records	Salary ledger card/records	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.24	Finance- Salaries and related records	Copies of salaries/wages payroll sheets	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.25	Finance- Purchase order records	Purchase order books/records	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.26	Finance- Purchase order records	Railway/courier consignment books/ records/Travel warrants	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.27	Finance- Purchase order records	Goods inwards books/records	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
7.28	Finance- Purchase order records	Delivery dockets, Stock/stores control cards/sheets/records	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.29	Finance - Financial Statements	Statements/summaries prepared for inclusion in quarterly/annual reports	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.30	Finance - Financial Statements	Periodic financial statements prepared for management on a regular basis	End of Financial Year	1 year	1 year	Destroy when cumulated into quarterly/annual reports	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.31	Finance - Asset register financial records	Assets/equipment registers/records	End of Financial Year	6 years after asset or last one in the register is disposed of	6 years after asset or last one in the register is disposed of	Review	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
7.32	Finance - Asset register financial records	Depreciation registers - Records relating to the calculation of annual depreciation	End of Financial Year	6 years after asset or last one in the register is disposed of	6 years after asset or last one in the register is disposed of	Review	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
8. Other Banking Records								
8.1	Other Banking Records	Cancelled / Dishonoured Cheque	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
8.2	Other Banking Records	Paid/presented cheques	End of Financial Year	6 years	7 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
8.3	Other Banking Records	Record of cheques drawn for payment	End of Financial Year	6 years	7 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
8.4	Other Banking Records	Bank deposit books/slips/butts	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
8.5	Other Banking Records	Bank deposit summary sheets - Summaries of daily banking	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
8.6	Other Banking Records	Bank reconciliations files/sheets	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
8.7	Other Banking Records	Bank statements, periodic reconciliations	End of Financial Year	2 years	2 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
8.8	Other Banking Records	Electronic banking and electronic funds transfer	End of Financial Year	6 years	6 years	Securely Destroy	HM treasury guidelines, National Audit Office advice	Legal compliance and best practice
9. Contracts and Agreements								
9.1	Contracts and Agreements	Contracts under seal and/or executed as deeds	Completion	12 years after completion (including any defects liability period)	12 years after completion (including any defects liability period)	Review	Limitation Act 1980.	Legal compliance
9.2	Contracts and Agreements	Contracts for the supply of goods or services, including professional services	Completion	6 years after completion (including any defects liability period)	6 years after completion (including any defects liability period)	Securely Destroy	Limitation Act 1980 (12 years if related to land).	Legal compliance
9.3	Contracts and Agreements	Documentation relating to small one-off purchases of goods and services, where there is no continuing maintenance or similar requirement	After purchase	N/A	3 years. Suggested limit: goods or services up to £10,000	Securely Destroy		Best practice.
9.4	Contracts and Agreements	Loan agreements	Last payment	N/A	12 years after last payment	Securely Destroy		Best practice
9.5	Contracts and Agreements	Licensing agreements	Expiry of agreement	6 years after expiry	6 years	Securely Destroy	Limitation Act 1980.	Legal compliance
9.6	Contracts and Agreements	Rental and hire purchase agreements	Expiry of agreement	6 years after expiry	6 years	Securely Destroy	Limitation Act 1980.	Legal compliance
9.7	Contracts and Agreements	Indemnities and guarantees	Expiry of agreement	6 years after expiry	6 years	Securely Destroy	Limitation Act 1980.	Legal compliance
9.8	Contracts and Agreements	Documents relating to successful tender	End of contract	N/A	6 years	Securely Destroy		Best practice

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
9.9	Contracts and Agreements	Documents relating to unsuccessful tenders	After notification	N/A	2 years after notification	Securely Destroy		Best practice
9.10	Contracts and Agreements	Forms of tender		N/A	6 years	Securely Destroy		Best practice
9.11	Contracts and Agreements	Documentation relating to purchases of medical devices and medical equipment		N/A	11 years	Securely Destroy		Best practice

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
10. Charitable Donations								
10.1	Charitable Donations	Deeds of covenant		N/A	12 years after last payment	Securely Destroy	TMA recommends 12 years after last payment. Limitation for legal proceedings if related to land.	Best practice
10.2	Charitable Donations	Index of donations granted		N/A	6 years	Securely Destroy	N/A	Best practice
10.3	Charitable Donations	Account documentation		3 Years	6 years	Securely Destroy	Companies Act recommends 3 years. Best practice	Best practice
11. Applications and Tenancy Records								
11.1	Application and Tenancy Records	Applications for accommodation	Offer accepted	N/A	6 years after offer accepted	Securely Destroy	Limitation Act 1980, section 2	Best practice
11.2	Application and Tenancy Records	Continuous Recording of lettings and sales (CORE) data record form		N/A	As long as it is deemed necessary to support social housing policy.	Securely Destroy	CORE Data Sharing Agreement 12.1	Best practice
11.3	Application and Tenancy Records	Housing Benefit notifications		N/A	2 Years	Securely Destroy	Recommendation from Chartered Institute of Housing. Good practice as per DWP guidance	Best practice
11.4	Application and Tenancy Records	Rent statements		N/A	2 years	Securely Destroy		Best practice
11.5	Application and Tenancy Records	Tenants' tenancy Files, including rent payment records, and details of any complaints and harassment cases		6 years	6 years' records plus current year	Securely Destroy	Limitations Act 1980	Legal compliance
11.6	Application and Tenancy Records	Former tenants' Tenancy Agreements, and details of their leaving	End of tenancy	6 years	6 years	Securely Destroy	Limitations Act 1980	Legal compliance
11.7	Application and Tenancy Records	Care plans for children and related documents		Until 75th year of child's birth or 15 years after death if child dies before 18. (Case records including care plans)	Until 75th year of child's birth or 15 years after death if child dies before 18. (Case records including care plans)	Securely Destroy	Arrangements for Placements of Children (General) Regulations 1999 and Children's Act 1989. Some documents may be transferred to subsequent caring agency.	Legal compliance
11.8	Application and Tenancy Records	Care plans/ case files for adults and related documents	End of support	8 years from end of care. (Adult Social Care)	8 years from end of care. (Adult Social Care)	Securely Destroy	Records Management Code of Practice for Health and Social Care 2016 Some documents may be transferred to subsequent caring agency.	Legal compliance
11.9	Application and Tenancy Records	Documentation, correspondence and information provided by other agencies relating to special needs of current tenants		While tenancy continues	While tenancy continues	Securely Destroy		Best pracice
11.10	Application and Tenancy Records	Records relating to offenders, ex-offenders and persons subject to cautions		While tenancy continues	While tenancy continues	Securely Destroy	NACRO	Best practice
11.11	Application and Tenancy Records	Safeguarding Referral		10 years	10 years	Securely Destroy	Statutory requirement under the Safeguarding Vulnerable Groups Act 2006 and Care Act 2014	Legal compliance
11.12	Application and Tenancy Records	Safeguarding Records - Serious Case Review		Minimum of 364 days or when notified Home Office has closed DHR	Minimum of 364 days or when notified Home Office has closed DHR	Securely Destroy	Records relating to child protection should be kept for 7 years after your organisation's last contact with the child and their family – NSPCC guidance	Legal compliance
12. Tenancy Records								
12.1	Property Records	Rent registrations (superseded)	Superseded document	N/A	6 years	Securely Destroy	Rent Officer Handbook recommendation	Best practice
12.2	Property Records	Rent Registration (not superseded)		N/A	Life of company	Securely Destroy	Rent Officer Handbook recommendation	Best practice
12.3	Property Records	Fair rent documentation		N/A	6 years	Securely Destroy	Rent Officer Handbook recommendation	Best practice
12.4	Property Records	Leases and deeds of ownership		N/A	15 years after expiry.	Securely Destroy	NCVO	Best practice

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
12.5	Property Records	Copy of former leases	Settlement of all issues	12 years	12 years	Securely Destroy	Limitation for legal action relating to land or contracts under seal. Limitations Act 1980	Legal compliance
12.6	Property Records	Wayleaves, licences and easements	Rights given or received cease	12 years	12 years	Securely Destroy	Limitation for legal action relating to land or contracts under seal. Limitations Act 1980	Legal compliance
12.7	Property Records	Abstracts of title	Interest ceases	12 years after interest ceases	12 years	Securely Destroy	Limitation for legal action relating to land or contracts under seal. Limitations Act 1980	Legal compliance
12.8	Property Records	Planning and building control permissions	Interest ceases	12 years after interest ceases	12 years	Securely Destroy	Limitation for legal action relating to land or contracts under seal. Limitations Act 1980	Legal compliance
12.9	Property Records	Searches	Interest ceases	12 years after interest ceases	12 years	Securely Destroy	Limitation for legal action relating to land or contracts under seal. Limitations Act 1980	Legal compliance

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
12.10	Property Records	Property maintenance records		6 years	6 years	Securely Destroy	Limitation for legal action relating to land or contracts under seal. Limitations Act 1980	Legal compliance
12.11	Property Records	Reports and professional opinions		6 years	6 years	Securely Destroy	Limitation for legal action relating to land or contracts under seal. Limitations Act 1980	Legal compliance
12.12	Property Records	Development documentation	Settlement of all issues	12 years	12 years	Securely Destroy	Limitation for legal action relating to land or contracts under seal. Limitations Act 1980	Legal compliance
12.13	Property Records	Invoices		12 years	12 years	Securely Destroy	Limitation for legal action relating to land or contracts under seal. Limitations Act 1980	Legal compliance
13. Vehicles								
13.1	Transport & Vehicles	Mileage records & defect sheets	Vehicle disposal	N/A	2 years	Securely Destroy		Best practice
13.2	Transport & Vehicles	Maintenance records & MOT tests	Vehicle disposal	N/A	2 years	Securely Destroy		Best practice
13.3	Transport & Vehicles	Copy Registrations	Vehicle disposal	N/A	2 years	Securely Destroy		Best practice
13.4	Transport & Vehicles	Vehicle disposal log	Vehicle disposal	N/A	1 year	Securely Destroy		Best practice
13.5	Transport & Vehicles - Operators Licence Only	Operators Licence certificates and documents of title	N/A	Permanently	Permanently	Securely Destroy	Driver & Vehicle Standards Agency (DVSA) Operators Licence requirement	Legal compliance
13.6	Transport & Vehicles - Operators Licence Only	Mileage records & defect sheets	Vehicle disposal	15 months	2 years	Securely Destroy	2 years is best practice. DVSA requirement to keep for 15 months under Operators Licence	Best practice
13.7	Transport & Vehicles - Operators Licence Only	Maintenance records & MOT tests *(up to 3.5T)*	Vehicle disposal	15 months	2 years	Securely Destroy	2 years is best practice. DVSA requirement to keep for 15 months under Operators Licence	Best practice
13.8	Transport & Vehicles - Operators Licence Only	Maintenance records & MOT tests *(HGV over 3.5T)*	Vehicle disposal	15 months	2 years	Securely Destroy	2 years is best practice. DVSA requirement to keep for 15 months under Operators Licence	Best practice
13.9	Transport & Vehicles - Operators Licence Only	Copy Registrations *(up to 3.5T)*	Vehicle disposal	15 months	2 years	Securely Destroy	2 years is best practice. DVSA requirement to keep for 15 months under Operators Licence	Best practice
13.10	Transport & Vehicles - Operators Licence Only	Copy Registrations *(HGV over 3.5T)*	Vehicle disposal	15 months	2 years	Securely Destroy	2 years is best practice. DVSA requirement to keep for 15 months under Operators Licence	Best practice
14. Capital Assets								
14.1	Capital Assets	Capital Assets including all land, property, housing stock, corporate buildings, play areas, vehicles, equipment, fixtures & fittings >£400	Asset sold, transferred or disposed of	N/A	6 years	Securely Destroy		Best practice
14.2	Capital Assets	Fixed Asset Register	NA	Permanently	Permanently	Securely Destroy	Charities Act	Legal compliance
15. Employees - Tax and Security								
15.1	Tax and Social Security	Record of taxable payments; record of tax deducted or refunded; record of earnings on which standard NI Contributions payable; record of employer's and employee NI contributions	End of Financial Year	Not less than 3 years after the end of the financial year to which they relate	6 years	Securely Destroy	HM Revenue and Customs requires retention of each payment for 3 years. Income Tax (PAYE) Regulations 2003 (SI 2003/2682 Reg 97). The Income Tax (employments) Regulations 1993 (SI 1993/744) and amended 1996	Legal compliance

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
15.2	Tax and Social Security	NIC contracted out arrangements; Inland Revenue notice of code changes, pay and tax details.	End of Financial Year	Not less than 3 years after the end of the financial year to which they relate	6 years	Securely Destroy	Income Tax (PAYE) Regulations 2003 (SI 2003/2682 Reg 97). The Income Tax (employments) Regulations 1993 (SI 1993/744) and amended 1996. Taxes Management Act 1970	Legal compliance
15.3	Tax and Social Security	Copies of notices to employees (e.g. P45, P60);	End of Financial Year	Not less than 3 years after the end of the financial year to which they relate	6 years plus current year	Securely Destroy	Income Tax (PAYE) Regulations 2003 (SI 2003/2682 Reg 97). The Income Tax (employments) Regulations 1993 (SI 1993/744) and amended 1996. Taxes Management Act 1970	Legal compliance
15.4	Tax and Social Security	HMRC notice of code changes, pay & tax details		6 years	6 years	Securely Destroy	Taxes Management Act 1970	Legal compliance
15.5	Tax and Social Security	Expense Claims	After audit	3 years from the end of the tax year they relate to	6 years	Securely Destroy	HMRC	Best practice
15.6	Tax and Social Security	Record of sickness payments	On payment	6 years	6 years	Securely Destroy	Taxes Management Act 1970 Inland Revenue require retention of each payment for 3 years. SSPR recommends 3 years following year to which they relate	Legal compliance
15.7	Tax and Social Security	Record of maternity payments, statutory paternity pay, statutory shared parental pay and statutory adoption pay	On payment	6 years	6 years	Securely Destroy	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended. The Statutory Paternity Pay and Statutory Adoption Pay (admin) Regulations 2002 (SI 2002/2820) and Statutory Shared Parental Pay (Admin) regulations 2014 (SI 2014/2929)	Legal compliance
15.8	Tax and Social Security	Income Tax and NI returns	End of Financial Year	Not less than 3 years after the end of the financial year to which they relate	6 years	Securely Destroy	Income Tax (PAYE) Regulations 2003 (SI 2003/2682 Reg 97). The Income Tax (employments) Regulations 1993 (SI 1993/744) and amended 1996	Legal compliance
15.9	Tax and Social Security	Redundancy details and record of payments & refunds	Date of redundancy	N/A	6 years	Securely Destroy	IPD recommended	Best practice
15.10	Tax and Social Security	Revenue and Customs approvals		N/A	Permanently	Securely Destroy	CIPD recommended	Best practice
15.11	Tax and Social Security	Annual earnings summary	End of Financial Year	N/A	12 years	Securely Destroy		Best practice
15.12	Tax and Social Security	Payroll/ salary records, overtime, bonuses expenses etc.	End of Financial Year	Not less than 3 years after the end of the financial year to which they relate	3 years	Securely Destroy	Income Tax (PAYE) Regulations 2003 (SI 2003/2682 Reg 97). The Income Tax (employments) Regulations 1993 (SI 1993/744) and amended 1996	Legal compliance
15.13	Tax and Social Security	Actuarial valuation reports		N/A	Permanently	Securely Destroy	CIPD recommended	Best practice
15.14	Tax and Social Security	Detailed returns of pension fund contributions; annual reconciliations of fund contributions		N/A	Permanently	Securely Destroy		Best practice
15.15	Tax and Social Security	Money purchase details	After transfer or value taken	N/A	6 years	Securely Destroy	CIPD recommended	Best practice

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
15.16	Tax and Social Security	Qualifying service details	After transfer or value taken	N/A	6 years	Securely Destroy	CIPD recommended	Best practice
15.17	Tax and Social Security	Investment policies	From end of benefits payable under policy	N/A	12 years	Securely Destroy	CIPD recommended	Best practice
15.18	Tax and Social Security	Trade Union agreements	Date of cessation	N/A	10 years after ceasing to be effective	Securely Destroy	CIPD recommended	Best practice
15.19	Tax and Social Security	Inland Revenue approvals		N/A	Life of company	Securely Destroy	CIPD recommended	Best practice
15.20	Tax and Social Security	Annual earnings summary	End of tax year	N/A	3 years from the end of the tax year they relate to	Securely Destroy	HMRC	Best practice
16. Human Resources - Pension Schemes								
16.1	Pension Schemes	Actuarial valuation reports		N/A	Permanently	Securely Destroy	CIPD recommended	Best practice
16.2	Pension Schemes	Detailed returns of pension fund contributions		N/A	6 years	Securely Destroy	Pensions Regulator	Best practice
16.3	Pension Schemes	Annual reconciliations of fund contributions		N/A	6 years	Securely Destroy	Pensions Regulator	Best practice
16.4	Pension Schemes	Money purchase details	After transfer	N/A	6 years after transfer or value taken	Securely Destroy	CIPD recommended	Best practice
16.5	Pension Schemes	Qualifying service details	After transfer	N/A	6 years after transfer or value taken	Securely Destroy	CIPD recommended	Best practice
16.6	Pension Schemes	Investment policies	End of benefits payable under policy	N/A	12 years	Securely Destroy	CIPD recommended	Best practice
16.7	Pension Schemes	Pensioner records	After benefits cease	N/A	12 years after benefits cease	Securely Destroy	CIPD recommended	Best practice
16.8	Pension Schemes	Records relating to retirement benefits	After transfer or value taken	N/A	6 years	Securely Destroy	RBS(IP)R recommended	Best practice
17. Human Resources - Personnel Records								
17.1	Personnel Records	Records relating to retirement benefits	After a year of retirement	N/A	6 years	Securely Destroy	RBS(IP)R recommended	Best practice
17.2	Personnel Records	Terms and conditions of service, both general terms and conditions applicable to all staff, and specific terms and conditions applying to individuals	Leaving date	N/A	6 years	Securely Destroy	Limitations Act 1980 Limitation for legal proceedings	Legal compliance
17.3	Personnel Records	Benefits and Deductions (Service contracts for directors (companies)	Date of cessation of directorship	3 years	6 years	Review	ICSA	Best practice
17.4	Personnel Records	Remuneration package	Leaving date	N/A	6 years	Review	Limitations Act 1980 Limitation for legal proceedings	Legal compliance
17.5	Personnel Records	Former employees' Human Resources files	Leaving date	N/A	6 years	Securely Destroy	CIPD recommended	Best practice
17.6	Personnel Records	References to be provided for former employees	Leaving date	N/A	6 years	Securely Destroy	CIPD recommended	Best practice
17.7	Personnel Records	Training Programmes	Leaving date	N/A	6 years	Securely Destroy	CIPD recommended	Best practice
17.8	Personnel Records	Individual training records	Leaving date	N/A	6 years	Securely Destroy	CIPD recommended	Best practice
17.9	Personnel Records	Short lists, interview notes and related application forms	Last Action	N/A	1 year	Securely Destroy	CIPD recommended	Best practice
17.10	Personnel Records	Application forms of non-short listed candidates	After notification	1 year	1 year	Securely Destroy	Limitations Act 1980 SDA & RRA recommend 3 months Commission for Racial Equality and Equal Opportunities recommends 6 months.	Legal compliance
17.11	Personnel Records	DBS certificate number	Date of clearance	Date of clearance + up to a maximum of 6 months	3 years	Review	DBS check code of practice (Home office)	Legal compliance Teign Housing hold only the certificate number but the system reminds HR to check again in 3 years.
17.12	Personnel Records	Time cards/ sheets	After audit	N/A	2 years	Securely Destroy	CIPD recommended	Best practice

Document overview			Retention Schedule					
Reference	Function	Record type	Retention trigger	Minimum statutory retention period	Recommended retention period	Action at end of retention period	Retention source	Reason for retention
17.13	Personnel Records	Trust deeds, rules and minutes (for joint employee/employer sports/social clubs, etc. set up under trust)		N/A	Permanently	Securely Destroy	CIPD recommended	Best practice
17.14	Personnel Records	Employer/Employee committee minutes (Staff Forum)		N/A	Permanently	Securely Destroy	CIPD recommended	Best practice
17.15	Personnel Records	Parental leave records	Birth of child	N/A	18 years from birth of child	Securely Destroy	CIPD recommended	Best practice
18. Human Resources - Health & Safety								
18.1	Health & Safety	Medical records relating to control of asbestos		40 years	40 years	Securely Destroy	The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632	Legal compliance
18.2	Health & Safety	Health and safety assessments; records of consultations with safety reps		Permanently	Permanently	Securely Destroy	Health and Safety at Work Act 1979	Legal compliance
18.3	Health & Safety	Health and safety policy statements		Permanently	Permanently	Securely Destroy	Health and Safety at Work Act 1979	Legal compliance
18.4	Health & Safety	Accident records, reports, accident books	Date of occurrence	3 years	6 years after date of occurrence/entry	Securely Destroy	RIDDOR Limitation for legal proceedings RIDDOR 1995 and Limitation Act 1980 Special rules apply concerning incidents involving hazardous substances.	Legal compliance
18.5	Health & Safety	Sickness records	Date of occurrence	3 years	6 years from date of sickness	Securely Destroy	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894) as amended Professional Standards Agency	Legal compliance
18.6	Health & Safety	Health and safety statutory notices	Once compliant	6 years after compliance	6 years after compliance	Securely Destroy	Limitations Act 1980 Limitation for legal proceedings	Legal compliance
19. Technical and Research Records								
19.1	Technical and Research	Technical and research records	After requirements have ended	N/A	12-15 years after requirements have ended for both records and reports and drawings and other data.	Securely Destroy	NCVO	Best practice
20. ASB case files and associated documents								
20.1	ASB case files and associated documents	ASB (Anti-social behaviour) case files and associated documents		N/A	5 years or until end of legal action	Securely Destroy		Best practice
21. Supporting people – subsidy claims / support plans / single assessments including supporting information								
21.1	Supporting People	Supporting people – subsidy claims / support plans / single assessments including supporting information		N/A	Duration of tenancy	Securely Destroy		Best practice
22. Resident Meetings								
22.1	Resident Meetings	Resident Meeting Minutes	From date of meeting	N/A	1 year	Securely Destroy	ICSA recommended	Best practice