Blackwood
homes | care | support

Data Protection Policy

Version Number	Issue 3
Date Revision Complete	May 2018
Policy Owner	Head of Business Services
Author	Governance & Information Officer
Reason for Revision	Reviewed in the context of new GDPR legislation
Proof Read	Yes – Governance & Assurance Manager
Date Approved	12th June 2018
Approved by	Board
Next Review Due	June 2021

Audience – Training and Awareness Method	Employees to be notified via briefing email and roadshows relating to GDPR.
Effective Date	12th June 2018

Internal References	Email and Internet Usage Policy Information Security Policy Openness & Confidentiality Policy Code of Conduct for Employees Code of Conduct for Board Members
External References	General Data Protection Regulations 2018

Appendices	

Comments:

Blackwood
homes | care | support

Data Protection Policy

1. POLICY STATEMENT

1.1 Blackwood recognises that the General Data Protection Regulations 2018 (GDPR) are important in protecting the rights of individuals in respect to any personal information that is kept about them, whether on computer or in manual filing systems. The aim of this policy is to ensure Blackwood complies with this legislation and understands fully its obligations under the GDPR.

1.2 Blackwood also acknowledges that from a regulatory perspective, and for the confidence of Blackwood customers, a Data Protection Policy will ensure that personal information given to Blackwood will be treated appropriately.

1.3 This policy acknowledges the right of access for individuals to information held about them and the right to stop or prevent processing likely to cause damage or distress, the right to compensation for unlawful processing, the right to data portability, and the right to be forgotten. These rights apply to all data including CCTV images.

1.4 Blackwood's Data Protection Officer is the Head of Business Services.

1.5 Blackwood is registered with the Information Commissioner as a Data Controller and our registration number is **Z5644613**.

2. PRINCIPLES

2.1 There are six Principles of Data Protection contained in the GDPR that can be referred to by anyone who has a role to play in the management of personal information in Blackwood. These are summarised below:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.2 Employees and Board Members will be informed about data protection issues and their individual rights through their induction processes. Fair Processing Notices are in place to help employees and Board Members understand the principles of Data Protection and how these are administered by Blackwood. These will be distributed with employee contracts along side DOI forms once a job offer has been made, and can also be found on the Blackwood website: http://blackwoodgroup.org.uk/blackwood-policies.

2.3 Compliance with this policy is a condition of employment with Blackwood and any deliberate breach of the policy may result in disciplinary action, which for serious or deliberate breaches may include dismissal. Knowingly breaching the provisions of the GDPR may also lead to legal action being taken against the organisation and individuals.

2.4 Fair Processing Notices are also in place for customers, and these will be distributed with Housing Application Forms or Care Customer Welcome Packs.

2.5 Any contractors completing work for Blackwood will be briefed on the importance of data protection at the outset, for example as it relates to safeguarding sensitive personal information on a customer. Data Sharing Agreements have been developed for this purpose and will be issued to all contractors along with the contract agreement.

2.6 All data/information processed by Blackwood is covered by this policy.

2.7 A list of data protection definitions referred to in the Regulations and this policy document is attached as **Appendix 1**.

3. KEY OPERATIONAL FRAMEWORK

3.1 Processing of personal data will be carried out where the data subject has given positive consent or there is a statutory requirement for that data to be given.

3.2 The request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

3.3 Individuals also have the right to withdraw their consent at any time. The withdrawal of consent will not affect the lawfulness of data processed before it is withdrawn. Prior to giving consent, the individual must be informed of this right to withdraw consent. Withdrawing consent must be as easy as giving consent.

3.4 As outlined in Appendix 2, details of the reasons why data is sought and the reasons for which it will be used will be stated on all relevant Blackwood forms as appropriate,

3.5 The processing of special categories of personal data will only be carried out with the individual's explicit consent. Special categories of personal data are defined at **Appendix 1**.

3.6 Data which has been provided to Blackwood, in confidence, by a third party such as employment references or tenancy reference cannot normally be disclosed to the data subject, unless the author of the data (third party) can remain anonymous, agrees to its release at a later date or it is reasonable to comply with the access request without the originator's consent.

3.7 Where personal information is held by Blackwood on customers, applicants, employees and other individuals, these people have the right to access the information, unless it is exempt under the General Data Protection Regulations. A Subject Access Request flowchart is attached as **Appendix 3**.

3.8 Where a request for information is received (this must be in writing, including email correspondence), Blackwood will respond to the request within one month. Where the request is provided by electronic means, the information requested shall be provided in electronic form, unless otherwise requested.

3.9 No charge will be made for requests for information. However, Blackwood reserves the right to make a charge of up to £10 for administrative costs for duplicate copies.

3.10 Blackwood is registered with the Information Commissioner and the Registration Form is held with the Business Services Team. The Head of Business Services shall ensure subsequent requirements for registration are complied with and will liaise with the Senior Management Team and other managers on the content of the registration.

3.11 Blackwood's Registration Pages on the Information Commissioner's Website can be found using the following link.: https://ico.org.uk/esdwebpages/search. Our Registration Number is **Z5644613**. These pages show the information we are legally entitled to process and who we can share this information with.

3.12 Blackwood periodically tests compliance with this policy to ensure that all managers and employees are following our Data Protection requirements. These checks are carried out by our Internal Auditors as part of our three-year Internal Audit Plan, or internally by the Business Services Team. Guidance on what is expected in relation to Data Protection can be provided by the Head of Business Services at any time should it be needed. This can include;

- **New Employees** – Awareness training will be provided at the induction arranged by the HR Team or local management as appropriate. A copy of this policy will be included in the Induction Policies Reading List, and can be found on the employee intranet, The Loop.
- **Existing Employees** – Ongoing training will be provided. This will be refreshed according to job role, with Managers receiving a greater number of refresher sessions. Managers will receive a refresher session annually. Other employees will receive a refresher session bi-annually. Data Protection is a subject that should also be discussed periodically at Team Meetings.
- **Board Members** – Members of the Board will have this policy made available to them through the BoardZone but can be provided with hard copies on request. New members of the Board are provided with awareness training as part of their induction process, which should include guidance on Data Protection and Openness & Confidentiality.

3.13 The following policy documents have been developed and implemented to ensure Blackwood's compliance with the principles of the GDPR as these apply to the day to day activities of Blackwood:

- Email and Internet Usage Policy
- Information Security Policy
- Openness & Confidentiality Policy
- Code of Conduct for Employees

- Code of Conduct for Board Members

4. RESPONSIBILITIES

4.1 The Head of Business Services is Blackwood's Data Protection Officer and, supported by the Governance and Information Officer, will be responsible for the following:

- Notification and registering with the Information Commissioner.
- Co-ordinating any amendments to Blackwood's registration.
- Monitoring and reporting to the Senior Management Team on compliance and any subject access rights or requests.
- Advising managers on audit procedures.
- Advising managers on Data Protection training for employees.
- Ensuring alignment of our Data Protection Policy with our Openness & Confidentiality Policy.
- Liaising with the Business Solutions Manager on matters relating to IT Security.
- Co-operating with the Information Commissioner as required, for example where there is a breach of data protection principles and acting as a point of contact for the ICO on issues relating to processing.

4.2 The Business Solutions Manager will be responsible for ensuring that storage of digital data, systems back up, storage and disposal of digital media and IT systems are secure and that all associated Business Solutions Policies and Procedures underpin and align with this Policy.

4.3 The Head of Business Services will assist in implementing the requirements of the GDPR by:

- Informing and advising all employees and data processors who carry out processing of their obligations under the Regulations.
- Providing advice on the data protection impact assessment and monitor its performance .
- Disseminating information relating to the GDPR to those with Data Protection responsibilities.
- Responding and co-ordinating requests from individuals to access personal information we hold about them, whether they be employees, customers or Board Members (prospective/past/present).

4.4 Each manager has specific responsibilities for safeguarding the personal and sensitive information held on data subjects within their team and complying with the provisions of this policy and the GDPR.

4.5 It is the individual responsibility of each employee and Board Member to ensure they comply with Blackwood's Data Protection Policy and these associated procedures.

5. SECURITY OF DATA

5.1 All employees are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third party.

5.2 All personal data should be accessible only to those who need to use it. All personal data must be kept:

- In a lockable room with controlled access.
- In a locked drawer or filing cabinet.
- If data is electronic then it should be stored on Network servers and not on local systems and have suitable security access levels applied, determined and monitored by the Information Security Owner (ISO) in accordance with Blackwood Information Security Policy.

5.3 Particular care should be taken of portable IT equipment, memory sticks etc which should be password protected to prevent unauthorised access. Where highly sensitive data is by necessity stored on memory sticks, these must be protected by Advanced Encryption Standard encryption and passwords strictly controlled by the ISO.

5.4 Special categories of personal data should not be kept on memory sticks or routinely taken from Blackwood premises on any form of removable media.

5.5 Personal data held on removable media such as CD/DVD media must be disposed of in accordance with the Blackwood Information Security Policy.

5.6 Care should be taken to ensure that PC monitors and Mobile Device Screens are not visible except to authorised employees and that computer passwords are kept confidential. PCs, Mobile Phones, Laptops and other mobile devices should not be left unattended without password protected screen savers and manual records should not be left where they can be accessed by unauthorised personnel. Employees are to operate a "clear desk" policy when finishing work each day. No confidential papers should be left on desks under any circumstances, nor should any personal information of customers or employees be displayed on notice boards within offices and care homes.

5.7 Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be disposed of as "confidential waste". All disposal of IT equipment will be managed by the Business Solutions Manager and in accordance with the Waste Electrical & Electronic Equipment (WEEE) directives and the Blackwood Information Security Policy thus ensuring data destruction and system security.

5.8 This policy also applies to employees who process personal data outside Blackwood premises, such as when working from home. Off-site processing presents a potentially greater risk of loss, theft, damage to personal data. Employees should take particular care when processing personal data at home or in other locations. Any loss of data from either Blackwood premises or off site must be reported to the Business Solutions Manager and Head of Business Services immediately.

5.9 Retention & Disposal

5.9.1 Blackwood discourages the retention of personal data for any longer than necessary. Considerable amounts of data are collected, and some data will be kept for longer periods than others, however every effort should be made to review the need to keep it and safely dispose of data as soon as possible. See **Appendix 4** – Retention of Records.

5.9.2 Teams and Information System Owners, will regularly review the data they will dispose of in accordance with data auditing procedures. Blackwood will comply with external guide lines on the retention of records where appropriate.

5.9.3 Personal data will be disposed in a way that protects the rights and privacy of data subjects (e.g. disposal as confidential waste, deletion from IT systems and backups).

6. CLOSED-CIRCUIT TELEVISION (CCTV)

6.1 Under the GDPR images captured through CCTV are classed as personal data.

6.2 Blackwood will consider several issues before deciding on the need to install a CCTV system. These include whether CCTV is an appropriate measure within data protection considerations and the Information Commissioners Guidelines, to address problems in a specific area. For example, improved external or internal lighting might be more effective at preventing anti-social behaviour problems then installing CCTV. Blackwood will also determine whether CCTV is an appropriate response to local issues considering whether customers are in favour of installing CCTV and what the cost

would be to install and maintain the system, bearing in mind this would be re-charged to tenants through service charges.

6.3 Where CCTV is in use, images will be treated as "data" in the same manner as paper or computer based information. The main purpose of collecting data from CCTV cameras is the protection of Blackwood customers, employees and the public, the prevention of crime or anti-social behaviour and to safeguard Blackwood property. Data from CCTV cameras may be used as evidence during criminal or other legal proceedings and may be passed to other agencies within the scope of our Registration with the Information Commissioner.

6.4 The number and type of cameras will also be carefully considered. Customers, visitors and employees should not feel uncomfortable by the presence of CCTV and it will not be used to monitor private areas such as inside an office or a customer's home. CCTV signage will be in place where CCTV is present.

6.5 Customer consultation will include discussing if there are alternative options, any underlying reasons why the need for CCTV has arisen, the number and positioning of cameras, secure image recording and storage facilities, who has access to recorded images and whether the system is temporary, permanent or subject to a period of review.

6.6 Once a decision has been agreed, Blackwood will arrange contractors to install and test the system and then to train local employees on its operation. The appropriate member of Senior Management Team will be responsible for ensuring that those on site are aware of our DP Policy, the proper use of the system and how to respond to requests for access to recorded data.

6.7 Monitoring and Recording

6.7.1 CCTV systems in use at Blackwood will not be monitored on a constant basis. Employees may check the system from time to time. However access will be restricted to ensure the maximum privacy for that personal data. Employees should not use the system for monitoring movements of people in and around developments. They would not be expected to respond to requests from other customers who, for example, may want to find out what time someone went out or came back into the housing development.

6.7.2 The CCTV monitor should not be in a position where images can be seen by members of the public. If a meeting is being conducted in an office where CCTV is monitored, the CCTV monitor should be switched off if there is a risk that unauthorised people would be able to view images on screen.

6.7.3 Images will be recorded on a time loop. This means that recorded images are not kept indefinitely and will be recorded over on a 14-day period. The length of time images are stored before being overwritten should be known to employees responsible for monitoring the system in order to respond to enquiries from customers.

6.7.4 Recorded images will be kept securely and employees should not access these without the permission of their manager and only for specific purposes related to the use of CCTV, i.e. crime prevention/detection or dealing with anti-social behaviour.

6.7.5 CCTV images are the property of Blackwood as the Data Controller.

6.8 Notification

6.8.1 It is the responsibility of Blackwood, through the Property Investment Manager to ensure that proper warning signs are sited in all areas covered by CCTV.

6.8.2 The sign should detail the purpose of using CCTV, who is responsible for operating the system (Blackwood), and who to contact (usually a telephone number) in the event of an enquiry. This may be the local Blackwood office or Blackwood Head office.

7. MONITORING AND REVIEW

7.1 Any breaches of this policy or associated procedures will be reported to the EMT annually in summary format together with details of the number of subject access requests and whether or not these access requests have been arranged within the time period set out by the GDPR.

7.2 This policy will be reviewed every 3 years, or earlier as required.

APPENDIX 1

Data Protection Definitions Used in This Policy

Data Controller – a person or organisation who decides how personal data is to be processed and for what purpose. Blackwood is the data controller, not individual employees.

Data Processor – an organisation or person who processes personal data for and on behalf of a controller.

Data Subject – data subject means an individual (not an organisation), who is the subject of personal data such as a customer, employee or Board Member.

Data (including manual data/relevant filing system) – information which:

a) is being processed by means of equipment operating automatically in response to instruction given for that purpose, such as information in Universal Housing (UH),
b) is recorded with the intention that it should be processed by means of such equipment;
c) is recorded as part (or with the intention that it should form part) of a relevant filing system (i.e. any set of information relating to individuals to the extent that, although not processed as in (a) above, the set is structured, whether by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to an individual is readily accessible); and
d) does not fall within paragraph a), b), or c) but forms part of an accessible record such as a health record, educational record and/or an accessible public record.

Examples of manual data that may qualify as structured manual files:

- Employee Files – applications forms, appraisal forms, disciplinary records, sickness records, supervision notes etc.;
- Care Customer records –referral forms, medical information, contact details etc.;
- Housing Records – application forms, waiting lists, rent accounts etc; and
- Contact Record Cards – lists of names and addresses, contact numbers etc.

Personal Data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Special Categories of Personal Data – includes the following:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;

- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person; Mental or physical health;
- Data concerning health or data concerning an individual's sex life or sexual orientation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

APPENDIX 2

Blackwood's Data Protection Statement and Fair Processing Notice/Data Sharing Agreement

The statement below may be added to Blackwood forms or documents as necessary to comply with the GDPR and any subsequent domestic Data Protection laws.

"Blackwood is registered with the office of the Information Commissioner. Blackwood is the Data Controller for the purposes of the General Data Protection Regulations and all subsequent applicable data protection legislation.

The information you provide will be treated in confidence and in compliance with all relevant data protection legislation.

We may pass the information to other agencies or organisations as required by law and in accordance with our Registration with the Information Commissioner.

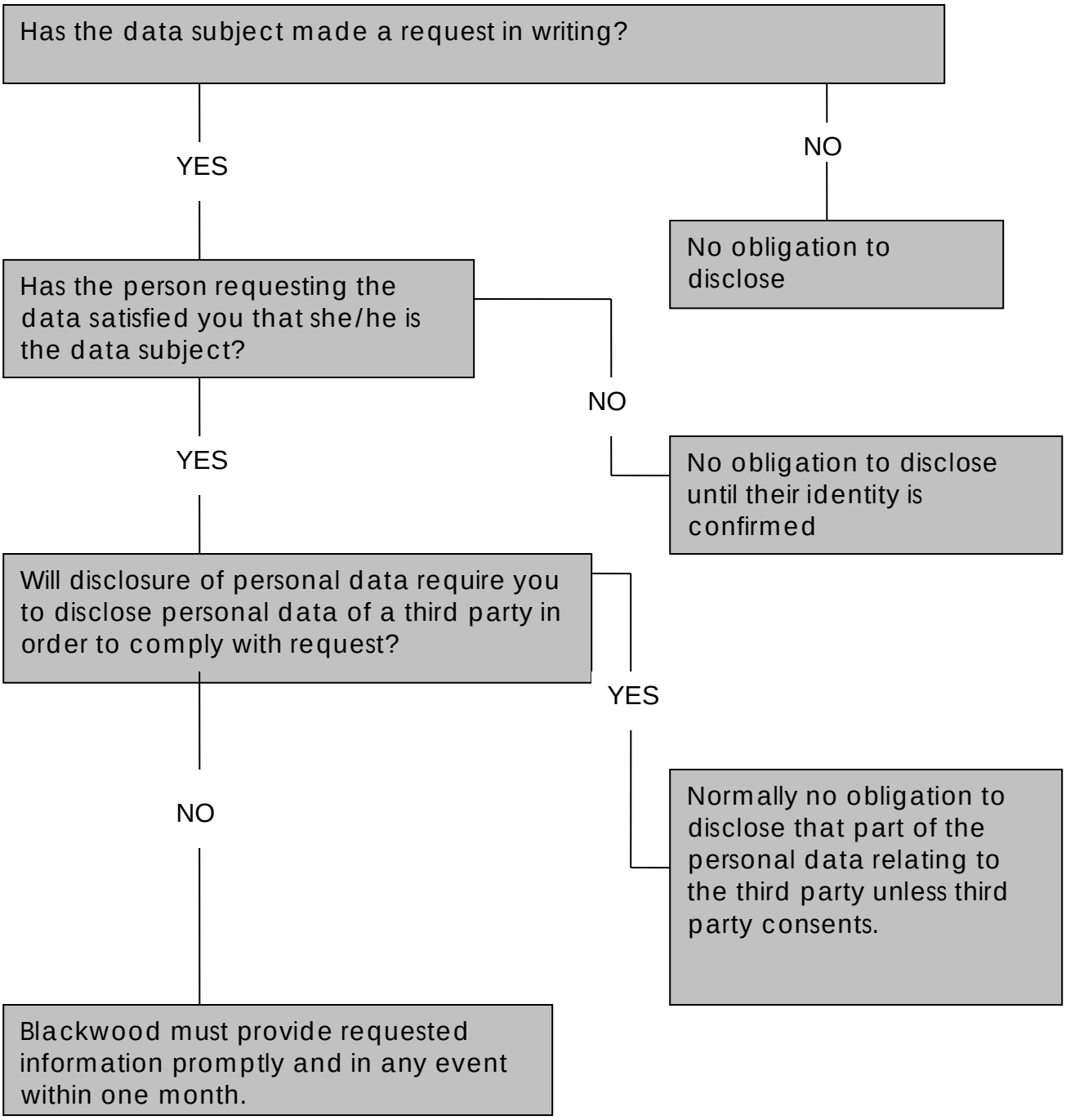
As the Data Subject you have the right to access the information we hold on you. If you wish to exercise this right, please contact our Head office in writing or via email with the details of your request."

Fair Processing Notices and Data Sharing Agreements will also be included in Blackwood's application and welcome packs as necessary to comply with the GDPR and any subsequent domestic Data Protection laws.

These documents are also available to view on the Blackwood website:
http://blackwoodgroup.org.uk/blackwood-policies

APPENDIX 3

Subject Access Request for Personal Data



APPENDIX 4

Retention of Blackwood Records

Blackwood processes personal data on a number of different subjects; these include customers, housing applicants, employees, applicants for employment and members of the Board of Blackwood.

We will ensure that all data is processed in accordance with the principles of Data Protection. We will comply with legislation and good practice advice wherever possible to ensure that data is kept only for as long as it is necessary for the purpose for which it is processed, and is securely destroyed thereafter.

All personal data will be retained securely for as long as it is required. Special categories of personal data, for example customer's medication records or financial circumstances, will be kept in recognised secure filing systems (either manual or electronic) with controlled access.

All personal data processed by Blackwood, under the definition in **Appendix 1** of this policy, is listed below with retention period and storage criteria. Other information, for example minutes of Board or Committee meetings, which falls under Company Law is omitted from this appendix.

Data Type	Manager	Retention Period & Reference	Storage
Care			
Current Care Customer Files	Care Service Manager	While active	Care Management Systems / Customer residence / Locked cabinet
Former Care Customer Files	Care Service Manager	6 Years from date of leaving	Care Management Systems / Off Site Storage / Locked cabinet
Medication Administration Records	Care Service Manager	2 Years (Information Governance Alliance Guidance 2016))	Customer file / Off site Storage / Locked cabinet
Housing			
Housing Applicant Data (Waiting List)	Housing Team Leader	Will only be retained whilst in use.	Locked cabinet / UH
Former Applicants	Housing Team Leader	1 Year from date of application	Locked cabinet / UH
Current Tenants Files	Housing Team Leader	Duration of tenancy	Locked cabinet / UH

Data Type	Manager	Retention Period & Reference	Storage
Former Tenants Files	Housing Team Leader	10 Years post tenancy	Locked cabinet / UH / Off Site Storage
Human Resources			
Employment Files, including copies of notices to employee (e.g. P45, P60)	Head of HR & OD	50 years after last date of payment of salary (Insurance Policy)	Electronic files
Redundancy details and record of payments and refunds	Head of HR & OD	12 Years (Charted Institute of Personnel and Development (CIPD))	Electronic files
Payroll Records – Tax and National Insurance, Maternity, Sick Pay/	Head of HR & OD	6 years (CIPD))	Electronic files
Application Forms, Interview Records	Head of HR & OD	1 year (CIPD)	Electronic files
Application Forms from non-shortlisted candidates	Head of HR & OD	6 months (IPD)	Electronic files
Return of pension fund contributions	Director of Finance	Permanently	Electronic files
Pension Records	Director of Finance	12 years after benefits cease	Electronic files
Inland Revenue Approvals	Director of Finance	Permanently	Electronic files
Disclosure documentation (e.g. PVG, DBS)	Head of HR & OD	Whilst in employment	Electronic files
Sickness records (sickness due to work conditions)	Head of HR & OD	6 years from end of sickness	Electronic files
Health and Safety			
Accident Records	Property Investment Manager	6 years after date of occurrence Records of Accidents & Incidents & Diseases that are RIDDOR reportable should be kept Indefinitely	Internal Accident Database

Data Type	Manager	Retention Period & Reference	Storage
Health and Safety Assessments and records of consultations with safety representatives	Property Investment Manager	Permanently	Electronic files
Sickness records (sickness due to work conditions)	Head of HR & OD	6 years from end of sickness	Electronic files
Business Solutions / IT			
Licencing Agreements	Business Solutions Manager	6 years after expiry	Electronic files.
Governance			
Board Member documents	Governance & Assurance Manager	6 years after Board membership ceases. Details such as bank details etc will be destroyed when membership ceases.	Electronic files
Membership documents	Governance & Assurance Manager	Permanently (Registrar of Friendly Societies)	Electronic files
Insurance			
Former and Current policies	Director of Finance	Permanently	Locked cabinet/ Electronic
Claims and related correspondence	Director of Finance	2 years after settlement	Locked cabinet/ Electronic
Files pertaining to possible cases of abuse	Property Investment Manager	50 years (Insurance Policy)	Electronic files / Locked cabinet
Property Management			
Contracts for supply of goods and services, including professional services and Rental and Hire purchase agreements	Property Investment Manager and Members of Executive Management Team	6 years after completion (including any defects liability period)	Locked cabinet/ Electronic
Contracts for the one-off supply of goods and services, where no continuing maintenance	Property Investment Manager	3 years after completion	Locked cabinet/ electronic
Documents relating to successful tenders	Property Investment Manager relating to property management	6 years after end of contract	Online portal/ Electronic

Data Type	Manager	Retention Period & Reference	Storage
Documents relating to unsuccessful tenders	Property Investment Manager relating to property management	2 years after notification	Online portal/ Electronic
General			
Contracts for the supply of goods and services	Relevant member of SMT.	6 years after completion	Locked cabinet/ Electronic