DATA PROTECTION & RETENTION POLICY

Contents

Version	Date	Owner	Details of Change
1.0	**July 2023**	**HR Director**	
2.0	**January 2026**	**Executive Leadership Team**	**Full review & update**

INTRODUCTION

We are committed to being transparent about how we collect and use the personal data of our residents and workforce, and to meeting our data protection obligations.

This policy sets out our commitment to data protection, and your rights and obligations in relation to personal data.

Borough Care has appointed Robert Jackson, CEO as the companies Data Protection Officer (DPO) who can be contacted by emailing Robert.jackson@boroughcare.org.uk.

SCOPE

This policy applies to employees working for Borough Care and all subsidiaries of Borough Care. Any reference to Company within this policy applies to all companies within the group and to all geographic areas in which homes are delivered.

DEFINITIONS

- **"Personal data"** is any information that relates to a living individual who can be identified from that information.
- **“Processing”** is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.
- **"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.
- **"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.
- **“Data Controller”** means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

DATA PROTECTION PRINCIPLES

The company is committed to being transparent about how it collects and uses the personal data of its residents and employees, and to meeting its data protection obligations.

This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR).

We will process all personal data in accordance with the following data protection principles:

- **Lawfulness, Fairness & Transparency**: We process personal data lawfully, fairly and in a transparent manner.
- **Purpose Limitation**: We collect personal data only for specified, explicit and legitimate purposes.
- **Data Minimisation:** We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- **Accuracy:** We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- **Storage Limitation**: We keep personal data only for the period necessary for processing.

- **Integrity & Confidentiality**: We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.
- **Accountability**: We take our data protection responsibilities seriously and comply with the Data Protection Act 2018.

The reasons for processing your personal data, how we use such data and the legal basis for processing is detailed in our Privacy Notice(s), which are included on our website and listed in Appendix 1 of this policy. We will not process your personal data for any other reasons.

There is stronger legal protection for more sensitive information, such as information about race, ethnic background, political opinions, religious beliefs, trade union membership, genetics, biometrics (where used for identification), health, sex life or orientation.

There are separate safeguards for personal data relating to criminal convictions and offences, and the information about how we store this information can be found in our DBS Policy.

TRAINING & AWARENESS

The company will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter through mandatory e-learning modules.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive training appropriate to their role to help them understand their duties and how to comply with them.

Data Protection and breach awareness will be discussed at employee meetings so that trends and patterns in potential data breaches can be reviewed and changes implemented where necessary. GDPR is a standing agenda item on the quarterly Safety Through Learning meeting which is chaired by the Director of Operations.

The company will maintain an Information Asset Register (IAR) and Register of Processing Activity (ROPA) which will be reviewed at least annually and involve relevant employees throughout the organisation to ensure that all data being processed has been identified and considered.

DATA RETENTION & DISPOSAL

The company will ensure that records are kept for the minimum statutory retention periods and will advise within this policy should we feel there is justification for retaining records for any further period of time.

The IAR and ROPA will contain more detailed information about how each piece of personal data is used, stored and disposed of and this will be reviewed at least annually.

Documentation	Reference	Retention Period
Social Care Records	The Health & Social Care Act 2008 The Care Act 2014	7 years after a resident has left our care
Personnel files	The UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (DPA 2018)	6 years after the end of employment
Training records	Health and Safety (First Aid) Regulations 1981 Fire Precautions (Workplace) Regulations 1997 Health and Safety (Consultation) Regulations 1996; Health and Safety Information for Employees Regulations 1989	6 years after employment – this covers statutory retention periods of 5 years for H&S training, and 6 years for First Aid Training and Fire Warden Training
Application forms/interview notes for unsuccessful candidates		1 year
Facts relating to redundancies where >20 are made redundant		12 years from redundancy date
All details concerning pay/salary	National Minimum Wage Act 1998. Taxes Management Act 1970 Working Time Regulations 1998 The Statutory Maternity Pay (General) Regulations 1986	6 years from the end of the tax year to which they relate. This includes the statutory requirement to keep NMW records for 3 years after the end of the pay reference period following the one that records cover. This also includes the statutory retention period of 2 years for working time records, and the

	Maternity & Parental Leave Regulations 1999 The Income Tax (Employments) Regulations 1993	statutory retention period of 3 years for maternity/paternity/parental and adoption records.
Accident books	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980	3 years from the last entry or until any younger person involved reaches 21 years old
Health records (as part of personnel records)		6 years
Whistleblowing documents	Public Interest Disclosure Act 1998	6 months following the outcome of a substantiated investigation. If unsubstantiated, personal data should be removed immediately.
Subject Access request	Data Protection Act 2018	1 year following completion of the request
Accounting records	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006	6 years

INDIVIDUAL RIGHTS

As a data subject, individuals have a number of rights in relation to their personal data.

Subject Access Requests (SAR)

The right of access, commonly referred to as subject access, gives (living) individuals the right to obtain a copy of their personal data from us, as well as other supplementary information. This is a fundamental right for individuals. It helps them understand how and why we are using their data and check we are doing it lawfully.

Individuals have the right to obtain the following from us:

- A copy of their personal data (if requested).
- Our purposes for processing.
- Categories of personal data we are processing.
- Recipients or categories of recipient we disclose personal data to.

- Our retention period for storing the personal data.
- The individual's right to request rectification, erasure or restriction or to object to processing.
- The individual's right to raise a complaint with the Information Commissioner's Office (ICO).
- Information about the source of the data, if we did not obtain it directly from the individual.
- Whether or not we use automated decision-making (including profiling) and information about the logic involved.
- The safeguards we have provided where personal data has or will be transferred to a third country or international organisation.

When responding to a SAR, we will supply this information in addition to a copy of the requested personal data itself. Usually, this information will be available within in our Privacy Statement and we will provide a copy of this along with the data.

Under the right of access, an individual is only entitled to their own personal data. They are not entitled to information relating to other people unless their data also relates to other individuals or they are exercising another individual's right of access on their behalf.

Before we respond to a SAR, we will assess whether the information we hold is personal data and, if so, to whom it relates.

How to make a SAR?

To make a subject access request, you should send the request to enquiries@boroughcare.org.uk. In some cases, we may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents it requires (see below section for further details).

We will normally respond to a request within 28 days from the date it is received. In some cases where the request is complex, we may require an additional 56 days to respond from the date it is received. We will write to you within 28 days of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing our organisation or causing disruption, or excessive where it repeats a request to which we have already responded.

If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether we will respond to it.

Who can make a SAR?

Anyone can request to see their own personal data if we have it. Sometimes an individual may prefer a third party (e.g. a relative, friend or solicitor) to make a SAR on their behalf. If this happens the data controller will make sure that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide us with evidence of this.

We will accept a written authority, signed by the individual, stating that they give the third-party permission to make a SAR on their behalf. The letter must contain the name and address of the individual as a minimum to enable us to be sure that they have given authority for the SAR. If we are

unable to satisfy ourselves that the request is genuine, we will write to the third party to explain why.

If the person about whom the information relates does not have the capacity to make a SAR for themselves, we will review requests from parties who have been legally appointed to act on their behalf, or we will follow a best interest process to determine whether we can share the requested data.

Access to Data for a deceased resident

If you require access to data about a decease person, the following procedure must be followed. Access to this information is not a SAR, but will be managed under the Access to Health Records Act 1990.

- Send the request to enquiries@boroughcare.org.uk.
- We will ask for proof of identification and will need to verify your relationship to the deceased. To do this we may request a copy of your passport / driving licence / bank statement or utility bill / grant of probate / certified will which lists you as an executor / letters of administration.
- We have 40 days to respond to your request once verification of your identity and relationship to the deceased is confirmed.
- If we are unable to provide the information requested, we will advise you of the reasons for refusal.

OTHER RIGHTS

You have a number of other rights in relation to your personal data. Individuals can require us to:

- Rectify inaccurate data.
- Stop processing or erase data that is no longer necessary for the purposes of processing.
- Stop processing or erase data if your interests override our legitimate grounds for processing data.
- Stop processing or erase data if processing is unlawful.
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether your interests override our legitimate grounds for processing data.

To ask the organisation to take any of these steps, you should send the request to enquiries@boroughcare.org.uk

DATA SECURITY

We take the security of personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

All company data is protected by file and folder permissions control. Access to company data requires a valid username and password that has been granted access to each particular area of data storage.

Where we engage with third parties to process personal data on our behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

IMPACT ASSESSMENTS

Some of the processing that we carry out may result in risks to privacy. Where processing would result in a high risk to individual rights and freedoms, we will carry out a data protection impact assessment to determine the necessity and proportionality of processing.

This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

DATA BREACHES

If we discover that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, we will:

- Report it to the Information Commissioner (ICO) within 72 hours of discovery by either calling the ICO Helpline on 0303 123 1113 for advice on how to manage the breach, mitigate the breach and to report the breach, or report online if we are confident that we are managing the effects of the breach and do not need advice (UK GDPR data breach reporting (DPA 2018) | ICO). We will record all data breaches internally regardless of their effect.
- Inform the affected individuals about the breach without delay.
- Inform the affected individuals about the steps we are taking to mitigate the effects of the breach and provide them with advice on what to do to protect themselves.

Employees will be made aware of what breaches should be reported to the Data Protection Officer (DPO) and a record will be kept which will be reviewed quarterly during our Safety Through Learning meeting.

All potential data breaches should be reported to the Executive Leadership Team for review. A decision will then be made as to whether the breach is reportable or not.

CYBER SECURITY & IT

The company is undergoing a review of its cyber security and will aim to be compliant with the Cyber Essentials Certificate. This policy will be updated when the identified requirements have been carried out.

In the meantime, the following security measures are in place.

- Cloud based file storage requiring password access.
- Laptops and desktop machines requiring password access.
- Permissions based file structure.

ACCOUNTABILITY

The Executive Directors assume overall responsibility for the implementation and adherence to this policy and, alongside the other senior managers, have legal responsibility for data protection matters. The Directors are responsible for:

- Ensuring that arrangements are in place for managing the processing of data, and holding the senior team accountable for lawful processing, SARs, training and awareness and reporting of breaches.
- Ensuring that there are sufficient resources for meeting the objectives of this policy.
- Ensuring that the Privacy Statement is reviewed regularly and up to date.

- Ensuring data protection is on the agenda for board level meetings and all cascade meetings throughout the organisation, including meetings at home level.
- Ensure that procedures are in place to monitor and review data protection processes and make subsequent required changes to policy and procedures are in place.
- Reviewing all potential data breaches before decision made on whether reportable to ICO or not.
- Reviewing the IAR and ROPA at least annually.

All employees must ensure that they follow our confidentiality procedures at all times. They must ensure that any personal data is stored securely and never shared with anyone who does not have the right to access it. Failure to observe this policy in its entirety may lead to disciplinary proceedings and result in potential dismissal. They must also:

- Comply with training, instruction and information that has been provided.
- Follow archiving and security processes in whichever part of the company they work.
- Report potential breaches immediately via email to a member of the Executive Leadership Team.
- Only access data that they have authority to access and only for authorised purposes.
- Never remove personal data or devices containing personal data from the company's premises.

LEGISLATION

You can find the full Data Protection Act 2018, and DUAA 2025 below should you wish to find further information.

Data Protection Act 2018

Data Use and Access Act 2025: plans for commencement - GOV.UK

COMPLAINTS

If you would like to make a complaint about how we are using your personal data please email enquiries@boroughcare.org.uk

We will acknowledge your complaint and respond to it without undue delay.

APPENDIX 1 – PRIVACY NOTICES

Please refer to individual privacy notices:

- Privacy Notice – Residents
- Privacy Notice – Relatives & Representatives
- Privacy Notice – Employees
- Privacy Notice - Applicants