DATA PROTECTION POLICY

Version Number	V4
Date of Current Version	December 2024
Approved by / Date	ELT / December 2024
Annual Review Date	April 2025
Full Review Date	April 2025

Executive Summary:
This policy describes RBH's approach to ensuring the personal data processed as a part if its operation is handled in a legal and safe manner.

Policy Grouping / Directorate	Corporate Services	
Owner Name / Job Title	Marcus Roe / Director of Governance	
Author Name / Job Title	Kevin Morgan / Risk and Compliance Manager	
Reviewed by Policy Team	Date: 5th Dec 2024	Name: Sarah Wilson
EIA Completed	Yes ☐	No ☒
Publication	Intranet ☒	Website ☒
Notes:		

1 Introduction and Aims

1.1 This policy outlines the considerations all Rochdale Boroughwide Housing (RBH) colleagues must take when handling personal data. it aims to protect fundamental rights and freedoms of Data Subjects.

1.2 The aims of the policy are:

- Ensure personal data is processed in a way that protects the data subject from harm.
- Provide a framework that allows RBH colleagues to process personal data in a way that is compliant with the data protection act.

2 Context

2.1 Taking robust measures to ensure the safe handling of personal data is a legal requirement under the Data Protection Act 2018 governed by the Information Commissioners Office. Failure to process personal data safely can cause harm to any individual whose data RBH handles.

Due to the potential severity of the harms that can arise from mismanagement of personal data, the ICO has set out the maximum fine for a data breach at £17.5 million or 4% of an organisation's total worldwide turnover, whichever is higher.

Management of personal data effects everyone, including RBH colleagues, customers and members of the public.

2.2 **Economic Standards**

This policy supports the achievement of the following economic standards:

Governance & Financing Viability Standard

There are a number of laws and regulations that apply to the processing of personal data. In order to adhere to the Governance & Financing Viability Standard, RBH must have a framework in place to ensure the relevant laws and regulations are not breached..

Consumer Standards

Transparency, Influence & Accountability Standard

Through the principles of data protection and the legal mechanism through which individuals can access their data, any organisation compliant with Data Protection Law will be transparent by default.

3 Values

3.1 The policy fits with the following mutual values of RBH:

Putting People First: We listen with empathy, respond with compassion, and make it easy for our customers to access our services.

The UK GDPR is a framework designed to ensure individuals safety is the number one priority. This can be seen through the requirements to ensure data security, transparency and accountability.

Doing What We Say: We earn trust through honesty, integrity, caring and keeping our promises.

The UK GDPR requires organisations to inform individuals how their data will be used prior to collecting it. It also provides a mechanism for individuals to review the data organisations have collected on them. This means that in order to comply with the legislation RBH must ensure we live up to our promises in regard to their personal data. This policy helps ensure we keep those promises.

Open & Transparent: We are curious, embrace diverse ways of thinking and seek feedback to help us improve.

Transparency is essential to ensuring organisations remain accountable to the individuals whose data they process. The UK GDPR incudes a set of rights that require organisations to be transparent about how they are using personal data.

4 Policy Statement

4.1 All colleagues have a responsibility for ensuring that when they are handling personal data, they do so in a safe and secure way.

The Data Protection Act 2018 and the UK GDPR sets out the requirements for the processing of personal data by organisations. This policy will provide details on the approach RBH will take when handling personal data to ensure it is handled appropriately.

Individuals have a number of rights under the data protection act. RBH will ensure that these rights are not infringed through the Data Protection Framework which encompasses:

- RBH's Record of Processing Activities.
- Data Protection Impact Assessments.
- Third Party and Supplier engagement and management.
- Subject Access Requests.
- Data Breach Management.

The approach to each part of the data protection framework is described in this policy.

4.2 Data Protection Officer

RBH employs a Data Protection Officer (DPO) whose role is to aid the organisation with Data Protection decisions and be a representative of the individual acting in a neutral capacity to ensure data is processed appropriately.

4.3 Handling of Personal Data

RBH colleagues will ensure that personal data is processed in accordance with the principles of data protection set out by the Information Commissioners Office (ICO):

- Lawfulness, fairness and transparency - Personal Data is processed with a genuine legal basis and, in a manner that ensures the data subjects rights.
- Purpose limitation - Personal Data is only used for the purpose it was gathered for.
- Data minimisation - No more data should be gathered, than what is needed to complete a specified task.
- Accuracy - Personal Data has measures taken to ensure its accuracy, preventing potential harms to data subjects.

- Storage limitation - Personal Data is stored for no longer than necessary to complete a specified task, and in line with laws and regulations.
- Integrity and confidentiality (security) - All appropriate measures are taken to ensure the security of the Data.

It is the responsibility of each colleague handling personal data to ensure they act safely and legally. All Personal Data processed in a department is owned by the Director, whose responsibility it is to ensure all processing of personal data in their department is done in an appropriate and legal manner.

4.4 **Data Protection Rights**

The Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR) give individuals rights over how their personal data is used.

- **The right to be informed**. Individuals have the right to know how and why their data is being used. RBH will ensure this right by providing details of how personal data is to be processed in its privacy policy, and where applicable using privacy notices.
- **Rights of access, portability and rectification**. Individuals have the right to access and receive a copy of their personal data and to ensure it is accurate and complete. This right will be ensured through responding in full to subject access requests. RBH's full approach is described at 4.11.
- **Right to erasure.** RBH will ensure that personal data is deleted in line with its retention policies. If an individual requests erasure, RBH will delete data where deletion is possible.
- **Right to object or restrict processing**. Individuals have the right to request that their personal data be restricted or suppressed and to object to how RBH is processing their data. RBH will review restriction requests and objections on a case-by-case basis.
- **Right not to be subject to automated decision making**. Individuals have the right not to be subject to a decision based solely on automated processing. Where RBH implements automated decision making, individuals will be notified and where necessary alternative options will be provided.

4.5 **Informing the Data Subject**

In order to ensure individuals, understand how RBH will process their data prior to collection, RBH will maintain a privacy policy that includes the general terms for handling personal data at RBH.

Some processes will deviate from the processing included in the privacy policy in order to achieve their stated aim. When this happens a privacy notice will be made available to the individual prior to data collection.

The privacy policy and privacy notices will inform the individual of everything they need to know to make an informed decision on whether to provide RBH with their personal data. Including but not limited to:

- The nature of the processing
- The purpose of the data required
- The legal basis for processing
- Where RBH will share the data

4.6 **Record of Processing Activities (RoPA)**

RBH will maintain a Record of Processing Activities (RoPA) as recommended by the ICO. This will identify all processing of personal data at RBH including:

- Which processes use personal data.
- Which department owns the personal data.
- Where personal data is gathered from, where it is stored and where it is sent.
- How long personal data is kept/retention periods.
- The legal basis for processing.

It will be the responsibility of each data owner to ensure that their processes that handle personal data are accurately recorded in the RoPA.

4.7 **Data Protection Impact Assessments (DPIA)**

RBH is required to process data in a high-risk manner to meet legal obligations and provide services that RBH is required to provide.

High-risk processing is:

- Processing involving the use of new technologies, or the novel application of existing technologies (including AI).
- Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special- category data.
- Any profiling of individuals on a large scale.
- Any processing of biometric data for the purpose of uniquely identifying an individual.
- Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.
- Combining, comparing or matching personal data obtained from multiple sources.
- Processing which involves tracking an individual's behaviour.
- The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
- Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.
- Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with the UK GDPR would prove impossible or involve disproportionate effort.

Where high-risk processing is required the data owner will ensure a DPIA is conducted to identify any further measures required to ensure the security and safety of personal data.

4.8 **Special Category Data**

Special category data is data that has been identified as having a potential to cause significant harms to individuals if it is exposed or gathered in large quantities.

As a social landlord RBH provides a number of services that require the processing of special category data to be effective. These include but are not limited to; assistance with money, managing antisocial behaviour, the provision of social housing and responding to complaints.

It is the responsibility of the data owners to ensure that where special category data is processed, all appropriate measures are taken to:

- Minimise the data used.
- Restrict the processing to only allow colleagues with a defined reason for processing the data to access it.
- Identify which security measures are required, beyond the standard measures for personal data.

The processing of special category data is inherently high risk. If a process includes special category data then it will aways need a data protection impact assessment in place.

4.9 Children's Data

Children under 16 are treated as vulnerable data subjects and additional care should be taken by data controllers when managing any child's data.

The processing of children's data is inherently high risk. If a process includes special category data then it will aways need a data protection impact assessment in place.

4.10 Data Sharing with third parties

If data is being shared with a third party on a frequent basis, then a data sharing agreement needs to be in place. RBH teams must understand their relationships with third parties and identify where they are sharing personal data.

Data owners with teams that manage a relationship with third parties are responsible for understanding if a Data Sharing Agreement is required, that it is implemented and RBH adheres to any requirements set out.

RBH will provide personal data to "Competent Authorities" as defined by the Data Protection Act 2018 in line with legal requirements.

4.11 Supplier Onboarding

RBH engages with third party suppliers through engagement by a lead officer who brings the third party though the procurement process.

A method to review the adequacy of each third-party supplier to process personal data will be in place, with the outcome readily available to teams using the supplier.

It is the responsibility of the data owner to ensure all third-party suppliers engaged by their directorate have adequate internal controls to process the personal data provided to them.

4.12 Subject Access Requests

Subject access requests are a key part of ensuring data protection integrity. Access to the data an organisation holds allows data subjects to ensure their data is being processed in the manner that the organisation stated prior to collection.

The Data Protection Act 2018 requires organisations to provide data subjects with a copy of the data held on them through the right of access. Data Subjects can make a subject access request through any official RBH channel. RBH will ensure there are clear channels through which data subjects can request a copy of their data and that all requests are handled within their statutory timeframes.

It is a requirement for organisations to complete a security check prior to fulfilling a SAR to protect data subjects. RBH will carry out appropriate security checks that do not obstruct the data subjects right to access their data.

When fulfilling a subject access request under the data protection act, RBH will adhere to the guidance provided by the ICO.

Some requests RBH receives may be classed as vexatious. Each request that is potentially vexatious will be reviewed by the DPO who will advise the appropriate action to take.

Individuals may request data from RBH through the Freedom of Information Act 2000. This act was implemented to ensure UK citizens were able to understand the actions that public bodies take. RBH is not a public body and not subject to the act, so will not provide data in a response to freedom of information requests. RBH reserves the right to provide data as a part of a response to a request at its discretion. Any response will not include personally identifiable information.

4.13 **Training and Awareness**

RBH will provide a comprehensive program of data protection training and awareness for all colleagues.

The training will be included as a part of the induction and refreshed every two years. The data protection training content will be reviewed annually. Team specific training will be provided where training needs are identified.

RBH will actively promote awareness of data protection requirements to colleagues frequently.

4.14 **Data Security**

The Data Protection Act 2018 requires organisations processing personal data to implement security measures that keep personal data safe. RBH will identify and implement appropriate security measures for each process.

RBH's full approach to data security is laid out in the IT Security & Acceptable Use Policy.

4.15 **Data Breaches**

A data breach is defined by the ICO as a security incident that has affected the confidentiality, integrity or availability of personal data. RBH will endeavour to prevent data breaches occurring, but if they do RBH will be resourced appropriately to manage them and prevent any harms to data subjects occurring.

Colleagues are required to complete annual training that provides the tools to identify data breaches. Colleagues will be responsible for ensuring they are able to identify a data breach when it occurs. Failure to report a data breach could lead to disciplinary action.

RBH will maintain and promote channels for the reporting of data breaches and will make sure the process is readily available for colleagues.

The Risk and Compliance team will take the lead in managing Data Breaches, following a documented process. The team will be resourced with the skills to identify whether a breach impacts the rights and freedoms of a data subject and therefore requires notifying the ICO. The team will also be responsible for ensuring the relevant stakeholders are aware of any relevant data breach.

If a data breach is significant enough that it requires notifying the ICO, the DPO and data owner must also be informed.

RBH will ensure that there is always a member of staff available who is trained to handle data breaches.

5 Monitoring

5.1 This policy is monitored through the following means:

- On an ongoing basis by the Data Protection Officer as a part of their responsibility to ensure they are kept informed of changes to trends, guidance and legislation.
- Regular reporting to the Service Leadership Team.
- Reporting key performance indicators to Audit and Risk Committee and Board.

6 Review

6.1 All RBH strategies, policies, service standards and procedures are reviewed on a regular basis to ensure that they are 'fit for purpose' and comply with all relevant legislation and statutory regulations.

6.2 This policy will go through the full policy approval process every three years and will undergo a desktop review annually. This is to ensure that it is fit for purpose and complies with all relevant and statutory regulations.

7 Links with Other RBH Documents

7.1 This policy links to the following policies and strategies:

- IT Security & Acceptable Use Policy
- Confidentiality Policy
- Data Strategy
- Digital Transformation Strategy
- Engagement Strategy
- Risk Management Strategy

8 Inclusivity Statement

8.1 We are dedicated to fostering an inclusive and equitable environment for all. We ensure that everyone is valued and respected. Our policies aim to be inclusive, and will comply with UK laws, including the Equality Act 2010, to create a diverse and supportive environment for people to thrive.

8.2 We understand not everyone absorbs information the same way. If you have any difficulty understanding or interpreting this document, please email people@rbh.org.uk or call Freephone 0800 027 7769. We will work with you to ensure your individual needs are met.