DATA PROTECTION & CONFIDENTIALITY POLICY

Version Number	V1
Date of Current Version	July 2025
Approved by / Date	ELT / August 2025
Annual Review Date	July 2026
Full Review Date	July 2028

Executive Summary:
This policy describes RBH's approach to ensuring the personal data processed as a part of its operation is handled in a legal and safe manner. This policy also ensures that RBH colleagues have guidance that allows them to manage confidential data in a safe and secure way.

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 June 2025	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 or confidential data. It aims to ensure confidential documentation is appropriately managed and to protect the fundamental rights and freedoms of Data Subjects (any identifiable person whose data is processed by RBH).

1.2 The aims of the policy are:

- Ensure personal data is processed in a way that protects the data subject from harm.
- Inform colleagues of their obligations in relation to confidential information.

2 Context

2.1 To carry out their roles, colleagues at RBH use and manage a range of information. In most cases such information will not be stated as confidential, and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential.

There will however be cases where information is confidential and requires extra measures and considerations to its processing.

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 Information Commissioners Office (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 confidential information 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.

Making sure that customers data is kept confidential unless necessary demonstrates that RBH is putting customers first. As a part of this approach 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.

Working As One: We embrace our mutuality and work together to deliver great outcomes for the people living in our homes and communities. The appropriate application of data protection legislation means RBH can engage more with customers and communities and achieve better outcomes without fear of causing harm to our customers through misuse of personal data.

Delivering Quality: We invest wisely in our people and make it easy for them to deliver services and create places that our customers are proud to call home. Keeping RBH colleagues informed on how to handle personal data means they can deliver services in a more effective manner and confidently use the personal data that is needed to complete their jobs.

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

RBH is transparent in its approach regarding data and will always explain what we will use personal data for and who if anyone we will share data with. As an organisation being clear about when information will not be disclosed allows interested parties to understand what information RBH will or will not disclose.

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 The Management of Confidential Information

4.1 This policy is intended to set out RBH's expectations to colleagues when handling any information as a part of their role at RBH. This includes but is not limited to any files or documents and colleague & customer personal data.

This policy instructs colleagues on identifying confidential information and managing it.

4.2 At RBH we define the different levels of confidentiality classification as set out below:

Public:

- Information that may be broadly distributed without causing damage to the organisation, its colleagues, and stakeholders. These documents may be disclosed or passed to persons outside the organisation.

For example this will include published information on websites, published policies, external communications material and published statutory returns.

Internal:

- The information meets the criteria for it to be kept out of the public domain.
- Unauthorized disclosure, particularly outside the organisation, would be inappropriate and inconvenient

This would include for example, Internal communications and publications, Policies and procedures, reports and briefing papers etc

Restricted:

- Improper disclosure of the information carries heightened risks
- There could be damaging consequences to RBH, Colleagues, Customers or the public, if it were lost, stolen or published in the media. In cases where there is a clear and justifiable requirement to share only on a need-to-know basis, the Sensitive classification must be used.

This would include for example, Board reports, Representative Body reports, strategies and action plans, ELT papers etc

Confidential:

- Improper disclosure of the information carries serious risks to the organisation and individuals.
- Information that must not be disclosed inside or outside of the RBH without the explicit permission of a member of the Senior Leadership Team.

This would include for example, confidential Board papers, personal employee information, financial information, legal documents etc.

4.3 **Colleagues Obligations**

- All confidential information must be kept secure at all times. It must not be taken outside RBH's systems or property, with appropriate measures taken to control access.
- Use of AI must adhere to the controls and restrictions set out in this policy. Colleagues must note that Microsoft CoPilot is not an RBH System. More detailed information relating to AI can be found in the Artificial Intelligence Policy.
- Confidential information must only be disclosed to others when authorised by senior management.
- RBH owned/controlled information must not be used for personal profit or benefit.
- Confidential information must not be replicated and stored on insecure devices.
- These restrictions will continue to apply even after the colleague has stopped working for RBH.

All personal data will be dealt with sensitively and in the strictest confidence internally and externally.

Digital controls for the management of information can be implemented in the systems RBH uses. If assistance is required to implement system access controls, then it is colleagues' responsibility to contact the IT Service Desk and manage the solutions they put in place.

4.4 Breaches of Confidentiality

RBH recognises that occasions may arise where individual workers feel they need to breach confidentiality. Confidential information as defined in section 4.2 may be divulged where there is risk of danger or where it is against the law to withhold it. For example, information may be divulged internally or to external agencies such as the police or social services.

Where a colleague feels confidentiality should be breached, they must raise the matter immediately with either their Line Manager, the Risk and Compliance Team or a member of SLT who will discuss the options available and decide whether confidentiality should be breached.

In some cases, a colleague will disclose confidential information, and the colleague they are disclosing it to will have a duty to report the information. Reporting this information to the appropriate individual is not a breach of confidentiality. The duty of confidentiality is always subject to the legal requirements of the Public Disclosure ("Whistleblowing") Act 1998, provided any disclosure is made in accordance with the provisions of this Act.

4.5 Wilful Breaches of Confidentiality

A colleague who wilfully breaches RBH's confidentiality guidelines may face disciplinary action under RBH's disciplinary procedures. The breach or breaches may constitute potential gross misconduct which may result in dismissal and legal action.

This policy is binding on individuals even after they have left RBH.

4.6 Categorisation of Confidential Information

Where colleagues manage information as a part of their role, they are responsible for determining whether it is confidential, and what level of confidentiality is required by this policy.

RBH uses the ISO27001 categories of confidentiality. This sets out levels of confidentiality and appropriate security measures.

If you are unsure what category applies to the information you are managing, contact your line manager to provide guidance.

RBH will ensure guidance on the handling of confidential information is available to colleagues, as well as providing reminders to colleagues on ensuring they meet the requirements in this policy.

5 Data Protection

5.1 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.

5.2 **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.

5.3 **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.

5.4 **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 5.12.

- **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.

5.5 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

5.6 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.

5.7 Data Protection Impact Assessments (DPIA)

There are occasions when RBH is required to process data in a high-risk manner to meet legal obligations and provide required services.

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.

5.8 **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.

5.9 **Children's Data**

Children under 16 are treated as vulnerable data subjects and additional care must 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.

5.10 **Data Sharing with third parties**

RBH will share personal data with third parties in order to meet its organisational aims and objectives. When sharing data with a third party it is recommended by the ICO to put a data sharing agreement in place. This allows RBH to set out the purpose and benefits of the data sharing, as well as who owns what data at every stage of a data sharing process.

Whilst data sharing agreements are only a recommendation by the ICO, RBH will ensure an agreement is in place if there is frequent data sharing. There will be instances where a one-off data transfer will pose a risk to RBH, either by the volume or nature of the data shared. In these instances, RBH would also expect a data sharing agreement to be in place.

It is the responsibility of the colleagues sharing the data to identify whether a sharing agreement is required, to ensure there is one in place and to adhere to the restrictions it imposes.

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

5.11 **Supplier Onboarding**

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

A method to review the adequacy of each third-party supplier to process personal data is 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.

5.12 **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 Subject Access Request (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 SAR 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.

RBH is not subject to the Freedom of Information Act 2000 as it is not classified as a public body for the purposes of the Act. As a result of this RBH 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.

5.13 **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.

5.14 **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.

5.15 **Data Breaches**

A data breach is defined by the Information Commissioners Office (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 training (see 5.13) 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.

6 Monitoring

6.1 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 Senior Leadership Team.
- Reporting key performance indicators to Audit and Risk Committee and Board.

7 Review

7.1 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.

7.2 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.

8 Links with Other RBH Documents

8.1 This policy links to the following policies and strategies:

- IT Security & Acceptable Use Policy
- AI Policy
- Data Strategy
- Digital Transformation Strategy
- Engagement Strategy
- Risk Management Strategy
- RBH Code of Conduct

9 Inclusivity Statement

9.1 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.

9.2 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.