DATA PROTECTION POLICY

Version Number	V2
Date of Current Version	October 2022
Approved by / Date	S Wigley / October 2022
Annual Review Date	October 2023
Full Review Date	October 2024

Executive Summary:
The Data Protection policy sets out how RBH protects personal data. It outlines the principles, rules and guidelines that all employees must follow when handling any data that could identify an individual. As a housing provider, RBH manages significant volumes of the personal data of our tenants and other customers as well as employee personal data. The policy gives guidance on collecting, storing and sharing personal data in a legal and responsible fashion. When handling personal data, employees are aware of who is responsible for the data, why RBH has it and who it can be shared with. It also outlines the steps that must be followed if a data breach occurs. All personal data held by RBH is done so as a part of a recorded process with a recorded legal basis.

Policy Grouping/Directorate(s)	Resources	
Author Name / Job Title	Data Protection Officer	
EIA Completed	Yes ☒	No ☐
Publication	Intranet ☒	Website ☒
Notes:		

1 Introduction

1.1 This Document outlines the Rochdale Boroughwide Housing approach to processes, procedures, and responsibilities that RBH colleagues must adhere to when handling personal data.

1.2 It outlines the principles, practices, and procedures RBH follows to ensure it complies with its legal duty to protect Data Subjects (an individual who is identifiable from the Data Processed by RBH), about the processing of personal data and rules relating to the free movement of personal data.

1.3 This Policy aims to protect fundamental rights and freedoms of Data Subjects and in particular their right to the protection of personal data.

1.4 Senior Managers who have ownership of personal data require a good knowledge of the whole Document. Other colleagues with specific information processing responsibility need a general grasp of the principles and knowledge of the procedures which they are regularly involved with.

1.5 For the sake of this Policy the words "information" and "data" are considered interchangeable.

1.6 All common processing is addressed in this document. It is recommended that the DPO is consulted if further in-depth information is required.

2 Context

2.1 Data Protection is a mechanism that allows organisations to demonstrate that they take the risk of any harms to individuals associated with them seriously.

3 Aims & Objectives

3.1 The aims of the policy are:

- Ensuring personal data is processed in a way that protects the data subject from harm.
- Documenting who is responsible for what in relation to handling personal data.
- Providing a framework that allows RBH members to work with personal data confidently.

3.2 The policy fits with the mutual values of RBH:

Responsibility – Individuals who are responsible for managing personal data are identified in this policy. RBH demonstrates its commitment to ensuring responsible handling of personal data.

Equity – This policy ensures that personal data is handled in a manner that ensures everyone's data is handled in the same way.

Democracy – This approach has been developed with each group it effects provided with the opportunity to have input.

Pioneering – This policy lays out how RBH is going to comply with a legal obligation.

Collaboration – This policy effects every department in the organisation, and so we will work with every department to ensure it is understood.

4 Policy Statement

4.1 What does good information Management look like at RBH?

4.1.1 Ownership

Colleagues are expected to take ownership of the data that they process on behalf of the Data Subject and to understand the measures required to keep data secure. They are able to identify where improvements are needed and ensure that these areas are brought to the attention of the listed Data Owners.

4.1.2 Principles of Data Protection

- **Lawfulness, fairness and transparency -** RBH ensures that Personal Data is processed with a genuine legal basis and, in a manner that ensures the data subjects rights. RBH also ensures that the Data Subject is aware of how their data will be processed.
- **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.
- **Accountability -** All Personal Data has an owner (Head of Service), whose responsibility it is to prevent harms coming to the Data Subject from their processing.

4.1.3 Security

All personal data has the appropriate level of security for the nature of the data processed.

Processes are designed with security in mind. Measures are taken to ensure that human error can happen without causing a data breach.

Access to personal data is appropriate and where necessary, restricted to those who have an appropriate legal basis for access.

Personal Data should not be stored on personal devices, or RBH devices without the appropriate security controls. Colleagues must use the storage solutions provided by IT, such as Office 365.

This Policy does not deal in detail with security of information i.e. the various physical and IT precautions taken to ensure data storage and processing systems provide the degree of security they are intended to. These can be found in the IT Security Policy 2021.

4.1.4 Colleague responsibility

All colleagues who handle personal data must pass the Data Protection training on a yearly basis.

All colleagues who handle personal data must be aware of the Data Assets they use.

All colleagues who handle personal data must be able to identify a Personal Data breach.

4.1.5 Training

Training is provided which enables RBH colleagues to work with personal data in a legal and secure manner.

4.2 Data Roles at RBH

4.2.1 Data Users

Personal Data is so integral to the way RBH operates, that all colleagues are classed as Data Users. Data users should:

1. Complete the training provided to ensure they understand the use of personal data, and their responsibilities to the organisation.
2. Communicate issues to Data Owners through Data Champions.
3. Understand the Data Assets they use that have Personal Data. Know what this means when handling that data.

4.2.2 Data Owners

Data Owners are heads of service at RBH. This is to ensure that they have the authority to make changes in their departments that can materially affect how data is handled.

They are responsible for the following:

1. Ensuring the data they are collecting is done so legally and in line with the principles of data protection
2. Implementing security and access to the data that is appropriate to its nature.
3. Maintaining the quality of data.
4. Ensuring that the Data Users who report to them are trained.
5. Reporting breaches internally to the DPO.

4.2.3 Director of Resources

The Director of Resources shall be accountable for the management of personal information within RBH so that compliance with data protection requirements and good practice can be demonstrated.

It is the Director of Resources responsibility to:

1. Ensure they have sufficient knowledge of information governance to be able to effectively oversee the delivery of data protection at RBH.
2. Ensure the contact details for the DPO are reported to the ICO.
3. Ensure the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
4. Provide the resources necessary for the DPO to carry out their responsibilities and to maintain their expert knowledge.

5. They shall not be dismissed or penalised for performing his tasks.
6. Ensure the DPO directly reports to the Board of Directors.

Ensure data subjects may contact the DPO about all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

4.2.4 Data Protection Officer

The role of the Data Protection Officer at RBH is to aid the organisation with Data Protection Decisions and be a representative of the Data Subject. It is important to remember that the DPO's tasks cover all personal data processing activities, not just those that require their appointment under Article 37.

The Data Protection Officers responsibilities are as follows:

1. Inform and advise RBH's colleagues about the obligations to comply with the GDPR and other data protection laws.
2. Monitor compliance with the GDPR and other data protection laws, and with RBH data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training colleagues and conducting internal audits.
3. Advise on, and to monitor, data protection impact assessments.
4. Cooperate with the supervisory authority; and
5. Be the first point of contact for supervisory authorities and for individuals whose data is processed (colleagues, customers etc).

4.3 Management of Data Assets

4.3.1 RBH controls its data through the management of Data Assets. Regarding personal data, each data asset holds the same definition as a Processing Activities do in the GDPR Article 4(2):

'processing' means 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.

4.3.2 Ownership of Data Assets

Data Assets are owned by the Head of service for the department that the Data Asset is controlled by. This is to ensure that the colleague who is responsible for using and protecting data can make material changes to the way it is handled.

Further requirements for data owners can be found in section 5. Data Roles at RBH.

4.3.3 Data Sharing

Data must not be passed to a 3rd party unless the sharing is specified in the Data Assets privacy notice prior to collecting the Personal Data.

If Data Sharing with a 3rd party needs to happen systematically, then a Data Sharing Agreement detailing the Personal Data shared must be in place prior to sharing.

4.4 Individual Rights

4.4.1 The Right to Rectification

The UK GDPR includes a right for Data Subjects to have inaccurate personal data rectified or completed if it is incomplete. It is for each colleague to ensure that they correct incorrect Data.

4.4.2 The Right to be Informed

RBH ensures that Data Subjects know what processing RBH carries out on their data using Privacy Notices. Where RBH is collecting personal data, the Data Subject is provided with where they can read what we will do with their data.

4.4.3 Rights managed by the Data Protection Officer

The Right of Access

Data Subjects have the right to receive a copy of the data that we hold on them. The primary channel for this is through a Data Subject Access Request (DSAR), for which we have an online portal (OneTrust). RBH will also respond to requests made through email, or via letter.

It is the Data Protection Officers responsibility to respond to DSARs.

The Right to Erasure

The Right to Restrict Processing

The right to data portability

The right to object

Rights in relation to automated decision making and profiling.

All of the above are to be assessed on a case by case basis, by the Data Protection Officer.

4.5 Freedom of Information Act

4.5.1 The organisation falls outside the remit of the Freedom of Information Act (FOIA) but there are circumstances where we hold information on behalf of other organisations that are covered by FOIA e.g. Rochdale Council. In cases where such organisations, in response to a Freedom of Information Request, ask RBH to provide data to them, RBH will send the requested information directly to the organisation dealing with the request not to the originator of the request.

4.6 Data Breaches

4.6.1 It is every colleague's responsibility to identify and report any Data Incident that could be a Data Breach.

Once reported, Data Breaches will be managed by the Data Protection Officer. Colleagues should use the Data Breach response form (appendix B) to report any potential breaches.

4.7 Data Mapping

4.7.1 RBH has an obligation to keep a record of all the personal data it uses.

The ICO has issued guidance on this subject that can be found here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

RBH meets this requirement through its Data Assets, which are effectively Processing Activities.

The Data Assets are held in OneTrust and reviewed on a yearly basis.

For further assurance, any changes to Data Assets are highlighted through the Data Management Forum.

4.8 Children's Data

4.8.1 Approach to Children's Data

RBH shall ensure special safeguards when collecting information directly from children.
RBH must obtain consent from the legal guardian for any profiling or marketing to children.
Data Subjects are no longer considered children once they have reached the age of 13.

4.8.2 Special measures for Children's Personal Data

Children under 13 are treated as vulnerable data subjects and additional care should be taken by data controllers when managing any child's data. To ensure the risks are fully understood a DPIA must be carried out. Any significant risks arising from this assessment must be appropriately managed to ensure no harms materialise.

4.8.3 RBH business which requires Children Personal Data

Whilst RBH does not directly provide services to people under the age of 13, there are several areas of business which do lead to Children's personal information being collected and processed. A non-exhaustive list is given below:

1. Tenancy Arrangements – collected for application for a home; tenancy support assistance given to tenants through completion of referral forms; provision of aids and adaptations; processing Right To Buy applications; processing of Homelessness Applications;
2. Work Experience / Employment Experience and After School Clubs – where RBH provides work experience opportunities, attends careers days, or has community clubs as part of its Community Partnership work.
3. Images & Video – as part of generation of corporate communications or provision of CCTV services.
4. Other Instances – such as for insurance claims or investigating/reporting claims of Anti-Social Behaviour.

4.9 Data Sharing

4.9.1 Transfer of Personal Information outside the UK

RBH does not normally transfer Personal Information outside of the UK. However should this be necessary (for example through cloud based data storage/processing), then prior to conducting any transfers the relevant Processing Activity Owner is to contact the DPO to ensure a Privacy Impact Assessment has been conducted and that adequate protections are in place.

4.9.2 **Disclosure to Third Parties requests**

Processing Activity Owners shall ensure that third parties provide evidence of:

1. their right to request a copy of the specified personal information; and
2. their right to request a copy of the specified personal information; and
3. where necessary, their identity.

The Processing Activity Owner is to check with the DPO, the legal grounds for disclosing any information to a third party. Only the minimum amount of personal information necessary shall be disclosed to third parties.

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.
- Through monitoring of transformation at RBH & the Data Integrity Board
- Through the documentation coming out of the Data Protection Forum

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 3 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 Policy

8 Appendices

A. Glossary
B. Data Breach Form
C. Annual Notification to ICO Procedure
D. Privacy Notice Procedure

Appendix 1

a) Glossary

Data Subject
A Data Subject is the identified or identifiable living individual to whom personal data relates.

Processing Activity
A Processing Activity is a set of operations performed on data to achieve a predesignated outcome.

Data Owner
A Data Owner is an employee of the organisation who is able to make decisions on how a Data Asset operates.

Data Champion
A Data Champion is an employee of the organisation who has a working knowledge of one or more Data Assets

Biometric Data
Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

Consent of the data subject
Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Controller
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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Controller in Common
The term "in common" applies where two or more data controllers share a pool of personal data, which they each process independently of one another. There may be multiple data controllers in respect of the same personal data.

Cross-Border Processing means either:
a) Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
b) Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Data Protection Officer (DPO)
Individual appointed by an organisation that has formal responsibility for data protection compliance.

Data Concerning Health
Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Enterprise
A natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

Explicit consent
Also known as express or direct consent — means that an individual is clearly presented with an option to agree or disagree with the collection, use, or disclosure of personal information.

Filing System
Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

Genetic Data
Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Information Society Service
A service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);

Joint Controller
Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

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;

Personal Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

PII & Sensitive PII
Personally identifiable information (PII), or sensitive personal information (SPI), as used in information security and privacy laws, is information that can be used on its

own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Privacy Notice
A privacy policy is a statement or a legal document (in privacy law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data.

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;

Processor
A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Profiling
Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Pseudonymisation
The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Recipient
A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Relevant and Reasoned Objection
An objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

Representative
A natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

Restriction of Processing

The marking of stored personal data with the aim of limiting their processing in the future;

Supervisory Authority

An independent public authority which is established by a Member State pursuant to Article 51; In UK this is the Information Commissioners Officer or ICO.

Third Party

A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Template Reviewed: 11th September 2020

REPORT OF DATA BREACH

Breach Reference:	
Date Incident Reported to DPO:	
Date of Incident:	

** All actions to be taken are identified (A#)*

1. CONTAINMENT

Inform the DPO immediately	
Has action been taken to limit the extent of the breach if possible? *e.g. isolate or close the compromised section of the network*	
Can losses be recovered to limit the damage the breach could cause? *e.g. recover documents if misdirected*	
Where the incident involves any form of theft or criminal activity, have the police been informed? *The police should be informed where individuals have deliberately accessed or copied data, as well as situations where records or equipment have been stolen*	
DPO to complete the Data Breach Template	

2. ASSESSMENT OF RISKS

Type of data is involved?	
How sensitive is the information involved?	
If data has been lost or stolen, are there any protections in place such as encryption?	
What could the data tell a third party about the individual?	
How many individuals' personal data are affected by the breach?	
Who are the individuals whose data has been breached?	
What harm can come to those individuals? *e.g. Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life.*	
Are there wider consequences to consider such as a risk to public health or loss of public confidence?	

3. CONSIDERATION OF FURTHER NOTIFICATION

Are there any legal or contractual requirements	
Can notification help the individual manage the risks? *e.g. by cancelling a credit card or changing a password (threshold is if there is high risk of adversely affecting individuals' rights &*	

freedoms)	
Who will RBH notify, what will they be told and how will the message be communicated?	
How can notification be made appropriate for particular groups of individuals? *e.g. children or vulnerable adults.*	
Who else should be notified? *e.g. third parties such as the police, insurers, professional bodies, bank or credit card companies.*	

4. EVALUATION AND RESPONSE

The DPO will meet with the relevant manager and satisfy RBH that it knows what personal data is held and where and how it is stored?	
In relation to the personal data involved in the breach, what and where are the biggest risks for RBH?	
Are the risks associated with the sharing or disclosing of data suitably identified & managed?	
What are the potential weak points in the RBH's current information security measures? *e.g. such as the use of portable storage devices.*	
Ensure that staff awareness of security issues is monitored and look to fill any gaps through training or tailored advice	

Head of Legal & Compliance Response	**Date:** Click here to enter a date.
RBH Director of Resources Response	**Date:** Click here to enter a date.
ICO Response from Verbal Notification	**Date:** Click here to enter a date.

Resulting Actions

Action	Owner	Target Date	Status

Information Management Framework Appendix E: Annual Notification to ICO Procedure

1 Purpose

1.1 The purpose is RBH and all subsidiaries are required to register with the Information Commissioner and renew this registration on an annual basis.

2 Scope

2.1 The timeframes to renew the registration are as follows;

RBH – renewal date 7th February annually
RBH Design and Build – renewal date 7th February annually
RBH Professional is currently dormant and so does not require registration.

3 Process

3.1 6 weeks before renewal the designated contact will receive an email notifying them of the need to renew. This is the Head of Legal and Compliance.

A letter is also sent.

3.2 The cost of registration depends upon the size of the organisation. There are 2 charging streams - £35 or £500.

3.3 The simplest way to renew is online and the Procurement Team will do this on our behalf using the company credit card.

3.4 Upon payment the ICO will then email a receipt to the designated contact confirming that the renewal has been completed and advising of the revised renewal date.

3.5 All documentation should then be saved by the Data Protection Officer in a suitable location.

Information Management Framework Appendix 11: Privacy Notices

1 Purpose

1.1 The purpose of this procedure is to set out RBH's approach to providing Privacy Notices to Data Subjects when and where RBH is collecting personal data for processing.

2 Scope

2.1 One of the Six Plus GDPR Principles is that personal information must be "***Processed lawfully, fairly and in a transparent manner***". This procedure addresses how RBH ensures transparency with the Data Subjects whose personal information is being processed by or on behalf of RBH.

The procedure covers:

- When personal information is collected directly from the Data Subject
- When personal information is collected via a Third Party
- How Privacy Notices are to be implemented at RBH
- How changes to are to be made to Privacy Notices

3 Introduction

Terminology

3.1 It is expected that the reader of this procedure will understand the following terms (should this not be the case please refer to the Appendix 16 – Glossary of Terms of the Information Management Framework):

- Data Subject
- Personal Data / Information
- Processing
- Data Protection Officer (DPO)
- Third Party
- Privacy Notice
- Privacy Information

When should a Privacy notice be provided?

3.2 When you collect personal data from:

- **The Data Subject** – you must provide a Data Subject with privacy information at the time you obtain their data.
- **A Third Party –** you need to provide the Data Subject with privacy information:
  - within a reasonable of period of obtaining the personal data and no later

than one month;

- if the data is used to communicate with the individual, at the latest, when the first communication takes place; or
- if disclosure to someone else is envisaged, at the latest, when the data is disclosed.

You must actively provide privacy information to individuals. You can meet this requirement by putting the information on your website, but you must make individuals aware of it and give them an easy way to access it.

You do not need to provide them with the same information more than once.

3.3 When obtaining personal data **from a third party**, you do not need to provide individuals with privacy information if:

- the individual already has the specific information;
- providing the information to the individual would be impossible;
- providing the information to the individual would involve a disproportionate effort;
- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
- you are required by law to obtain or disclose the personal data; or
- you are subject to an obligation of professional secrecy regulated by law that covers the personal data.

Any decision not to provide privacy information must be approved by the DPO. In instances where the information has already been provided there must be evidence to demonstrate this.

What does a Privacy Notice need to include?

3.4 GDPR Legislation sets out what should be contained within a privacy notice in two specific instances:

a) When personal data/information is obtained directly from the data subject

b) When personal data/information is obtained from a third party

These requirements are set out below:

What information do we need to provide?	Personal data collected from individuals	Personal data obtained from a third party
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓
The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	
The details of the existence of automated decision-making, including profiling	✓	✓

Methods of disseminating Privacy Notices

3.3 Privacy Information provided must be:

- concise,
- transparent,
- intelligible,
- easily accessible, and
- must use clear and plain language.

If necessary a separate version must be provided which can be comprehended by children.

3.4 It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.

For instance at a particular instance of data collection by providing a short Privacy Notice specific to the data being a collected but then having a separate comprehensive Privacy Policy which gives more detailed information regarding how data subjects may exercise their rights and RBH's personal data management.

3.5 Since in Personal Information in collected in many different mediums, different methods are needed to deliver the Privacy Notices. Thought also needs to be given to be give to how Privacy Notices are to be presented to data subjects. The table below sets out the main methods:

Medium	Method
Email / Letter	Privacy notice to be provided in the text of the email with a link / web address to the privacy policy
Websites	Cookie notification
Webforms	Privacy Notice text adjacent to the webform with a link to the Privacy Policy
Telephone	Read out the Privacy Notice and offer to provide any further detail from within the Privacy Policy
Paper Form	Privacy Notice text printed on the same page as the form with a the web address for the Privacy Policy
Face to Face	Read out the Privacy Notice and offer to provide any further detail from within the Privacy Policy. Have a paper copy of each available to give the data subject if requested.

When developing Privacy Notices, the practicalities of disseminating them should be considered as well as continually considering the ability of the Data Subject to understand the information being presented.

4 Procedure

Responsibilities

4.1 Processing Activity Owners are responsible for ensuring Privacy Notices are in place for their respective activity.

4.2 Where the data being collected at a particular instance is for more than one Processing Activity then a combined privacy notice is to be provided. One respective Processing Activity Owner is to co-ordinate the development and implementation of the Privacy Notice. The other Processing Activity Owners are not relieved of their responsibility to ensure a suitable privacy notice is in place.

4.3 Getting the right to be informed correct helps you to comply with other aspects of the GDPR and builds trust with people, but getting it wrong leaves RBH open to fines and reputational damage.

The provision of a Privacy Notice and Privacy Policy

4.4 A specific privacy notice is to be immediately apparent at the point of data collection.

4.5 An RBH wide Privacy Policy is to be accessible at the point of collecting personal data/information should a data subject wish to have more information on exercising their data subject rights and RBH's privacy management procedures.

Recording

3.9 The DPO maintains a register of RBH Privacy Notices. Historic Privacy Notices must be kept on record so that it can be determined what privacy information was provided to the data subject and when.

Developing the Privacy Notice

4.6 The key steps are:

a) Whatever the medium the Privacy Notice should have a similar format and wording. A template is provided at Annex A.

b) To find the specific details to be inserted into the template ask the DPO to extract the relevant information from the RBH Data Inventory. The DPO will need a list of the all the Processing Activities the Privacy is due to cover. *The Data Inventory will have been previously populated by the Processing Activity Owner having completed a Processing Activity Questionnaire.*

c) Populate the template and submit to the DPO for approval and adding to the Privacy Notice Register.

d) Implement the Privacy Notice in keeping with the medium by which the data is being collected (see "Methods of disseminating Privacy Notices"

above).

e) Ensure the RBH Privacy Policy is made accessible as set above.

f) If the Privacy Notice is for instances where the personal information was obtained from a third party, ensure the necessary notice is shared with the respective Data Subjects. A record should be made that the Privacy Notice was provided.

g) Consider user testing which is a good way to get feedback on how effective the delivery of your privacy information is.

Changes to the Processing Activity

4.7 Privacy Notices will be reviewed and where necessary updated at least annually.

4.8 If you plan to use personal data for a new purpose, the privacy information must be updated and the changes communicated to individuals before starting any new processing.

4.9 Changes to Privacy Notices are to be approved by the DPO and added to the Privacy Notice Register.

Monitoring

4.10 The DPO will regularly undertakes information audits to find out what personal data we hold and what we do with it.

4.11 When preparing privacy notices for a Processing Activity for which you are responsible, put yourself in the position of the data subject from whom information is to be collected.

5 Conclusion

5.1 This procedure sets out the means by which RBH ensures it is transparent with regard to the Personal Information Processing it carries out.

5.2 Transparency is ensured through the use of concise, transparent, intelligible, easily accessible, clear and plain language Privacy Notices and a RBH Privacy Policy.

5.3 The procedure has set out how the information notices are to contain, when and how they are to be produced, recorded, reviewed and monitored.

5.4 At the Annexes is a template Privacy Notice and the RBH Privacy Policy.

Annexes

1. Template Privacy Notice
2. RBH Privacy Statement