CONFIDENTIALITY POLICY

Version Number	V2
Date of Current Version	April 2023
Approved by / Date	Stephen Wigley / April 2023
Annual Review Date	April 2024
Full Review Date	April 2025

Executive Summary:
We deal with a large volume of confidential information which quite often relates to individuals, so there will be a significant amount of overlap with the Data Protection Policy. Although this is not always the case - such as where we hold information which may be financially or commercially sensitive but hold no personal information. This could include information about rates agreed under a procurement exercise. This policy gives guidance on what sort of information should be considered as sensitive, and what steps should then be taken to ensure this is treated with the required confidentiality.

Policy Grouping/Directorate(s)	Resources	
Author Name / Job Title	Kevin Morgan – Risk and Compliance Manager (DPO)	
EIA Completed	Yes ☒	No ☐
Publication	Intranet ☒	Website ☒
Notes:		

1 Introduction

1.1 This Document describes how to identify and manage confidential information at RBH.

2 Context

2.1 This policy has been developed to ensure the limitation, where necessary, of the use of information to only authorized persons i.e. the maintenance of privacy.

2.2 All colleagues have a responsibility to identify confidential information and follow the correct practices to ensure it is secure. All common processing is addressed in this document. It is recommended that the DPO and/or Legal are consulted if further in-depth information is required.

2.3 Whilst RBH is already obliged to release certain information under the Mutual Rules, the Data Protection Act 1998 and in accordance with the Homes and Communities Agency (HCA) 2015 Regulatory Framework for registered providers of housing, RBH goes further than these requirements in keeping with the RBH values.

3 Aims & Objectives

3.1 The aims of the policy are: To ensure that all RBH colleagues are able to identify confidential information and know what measures are required when handling confidential information.

3.2 The policy fits with the mutual values of RBH:

- Responsibility – Individuals have the responsibility for ensuring that the information they handle has the correct access restrictions.
- Equity - This policy will help ensure a fair environment for all employees, ensuring they know what information they can share and what they should not.
- Democracy - This approach has been developed in partnership with members.
- Pioneering - This policy supports a forward thinking approach to ensuring confidentiality in a mutual.

4 Policy Statement

4.1 Outline

RBH processes large quantities of information which whilst not relating to data subjects, is commercially sensitive; its uncontrolled processing could jeopardize an area of RBH business or an opportunity for business. For example, information relating to the procurement and contracts for goods and services.

- breach of laws, contracts, standards and frameworks;
- negative impacts on the choices, risks and opportunities facing RBH;

- physical, material or non-material damage to RBH including financial loss;
- reputational damage to RBH;
- regulatory action against RBH.

4.2 Classification of Commercially Sensitive information

Classification - The author/creator of any piece of RBH business information is responsible for determining whether or not it is confidential as required by this policy. If it is, the author becomes responsible for treating the material.

In the event there is uncertainty as to whether certain information is confidential then a colleague will contact their line-manager.

Classifications apply to all information at RBH including contents of meetings, members meetings and interactions with consultants etc.

Commercially Sensitive information is classified into three categories:

Category	Description
Public or open	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. Where the public is the intended audience, the information must go through the Communications Team.
Internal or proprietary	Information whose unauthorized disclosure, particularly outside the organisation, would be inappropriate and inconvenient.
Confidential or restricted	Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed inside or outside of the RBH without the explicit permission of a Head of Service.

If you are unsure how to classify information, then please consult the Head of Legal and Compliance or Data Protection Officer.

Information that contains no personal, sensitive personal or Corporate/Commercially Sensitive information, will be treated as public information.

Declassification - Sometimes due to changes in circumstance information that is classified Confidential or Internal ceases to be classed as such. In this situation the original author will be contacted and asked whether the information can be declassified. If so the information will then be treated as public information.

4.3 Handling Confidential Information

Information which is classified as Confidential can be recorded digitally or on paper and communicated in different ways. Whilst transferring/communicating information, correct security measures must be put in place to ensure confidentiality is maintained.

Further details of these measures are in Section 5 and the IT Security Policy.

Failure to take responsibility for correctly handling RBH information will result in disciplinary action.

4.4 Sharing Confidential Information

It is important that authors and authorised handlers of information do not unnecessarily designate information as confidential and put in place unnecessary barriers to the sharing of information. For information that is correctly designated confidential, the following measures must be adhered to:

i. Internal Sharing- Sharing of confidential information between colleagues of RBH should be strictly on a "need to know" basis, e.g. HR team sharing details of a health issue with their manager or gathering information for disciplinary investigations.

ii. External Sharing - There are circumstances where it is necessary to exchange information with other agencies without the consent of the individual concerned; for example to prevent or detect crime; when there is a legal requirement to share this information or if the safety of an individual is at risk; where RBH and the other organisation share common objectives; the other organisations requires the information in order to deliver a contract for RBH.

In a similar manner to sharing personal information externally, Commercially Sensitive Information must only be shared externally once there is a written agreement in place. This might be within a contract, data sharing agreement or by a requirement of law. In each case the Data Protection Officer must have a formally approved written record of the document before sharing is to take place.

Anyone unsure as to whether it is permissible to share information or not should seek advice from their line manager in the first instance or through the DPO

4.5 Breach of Confidentiality

In the event that any RBH colleague, Board member, Representative, supplier, partner or other RBH stakeholder becomes aware of classified information falling into or potentially falling into the possession of one or more people not entitled to have access to it, they are to alert the DPO immediately and refer to any actions that may be required.

4.6 Access Control

It essential that commercially sensitive and personal information held by RBH or on behalf of RBH can only be accessed by those with a need to access it. By minimising access to those who need access, risk of a breach of confidentiality or data protection is minimised.

RBH will minimise access by the following;

- The Data Asset Owner placing in restrictions as agreed one their Processing Activities
- The Data Asset Owner then further placing in controls agreed in the ISO 27002 document Appendix C.
- Folder Owners contact IT Service Desk to request instruction on how to set up access permissions in O365.

- Document Owners placing passwords on documents and distributing to only the necessary people.
- All colleagues to check what information they are sending out either by email or post and ensure that they are doing do securely.

Any queries to DPO@rbh.org.uk

For further information on IT Security at RBH, see IT Security Policy.

4.7 Members Meetings

- Members meetings are either Annual Members' Meetings (AMM) or Special Members' Meetings (SMM). RBH holds the Annual Members' Meeting within six calendar months after the close of each financial year or such later date as may be allowed by law.
- Members Meetings are open to all Members, Associates, Representatives and Directors, and the Auditor, all of whom have the right to speak.
- The Chair of the Board, will chair the meeting. If they are unable to do so a Chair will be elected at the start of the meeting.
- All members are invited to the AMM). In advance of the meeting Members can request a copy of the Annual Financial Statements and the Representative Body annual report to Members. The agenda, reports, and minutes for AMMs can be found online.

5 Monitoring

5.1 Use of the policy is monitored by the Data Protection Officer, confidentiality issues are included in the assurance report to ELT, Audit 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 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:

- Data Protection Policy
- Open Meeting Guidelines
- Confidentiality Report Cover Sheet