RBH

ALL TOGETHER BETTER LIVING

# DATA PROTECTION AND INFORMATION SECURITY POLICY

# DOCUMENT CONTROL

| | |
|---|---|
| **Document Reference / Version Number** | **Version 3 – December 2016** |
| **Title of Document** | **Data Protection and Information Security Policy** |
| **Authors Name(s)** | **Stephen Wigley** |
| **Authors Job Title(s)** | **Head of Legal and Compliance** |
| **Directorate(s)** | **Resources** |
| **Document Status** | **Final** |
| **Supercedes (Version & Date)** | **Data Protection and Information Security Policy 2015** |
| **Approved By** | **EMT (Formal review) and Head of Legal & Compliance (First Annual review)** |
| **Date of Approval** | **17th December 2015 and 23rd December 2016** |
| **Publication / Issue Date** | **December 2015** |
| **Date of Annual Review** | **December 2017** |
| **Changes Made at Last Review** | **None required** |
| **Full Review Date** | **December 2018** |
| **Distribution** | **Website and Intranet** |
| | |

Rochdale Boroughwide Housing Limited is a charitable community benefit society.
FCA register number 31452R.
Registered Office: Sandbrook House, Sandbrook Way, Rochdale OL11 1RY.
Registered as a provider of social housing. HCA register number: 4607


# CONTENTS


| Section | Page |
|---|---|
| Introduction | 4 |
| Statement of Policy | 4 |
| What is Data Protection | 4/5 |
| The Principles of Data Protection | 5/6 |
| Personal and Sensitive Personal Data | 6 |
| Handling of Personal/Sensitive Data | 6-8 |
| Subject Access Requests | 8 |
| Circumstances Where Personal Data May Not Be Released To An Individual | 9 |
| References to Other Individuals | 9 |
| Requests for Information from a Third Party | 9/10 |
| Employee Training | 10 |
| Information Security | 10/11 |
| Retention Periods | 12 |
| Surveillance Systems | 12-14 |
| Implementation | 15 |
| Complaints | 15 |
| Notification to the Information Commissioner | 15 |
| Equality and Diversity | 16 |
| Links to other RBH Strategies and Policies | 16 |
| Monitoring and Review | 16 |
| Appendix 1 – Glossary of Terms | 17-18 |
| Appendix 2 – Reporting Information Security Breaches | 19-21 |
| Appendix 3 – Categorising Serious Incidents Requiring Investigation | 22-23 |
| | |

## 1. Introduction

1.1 The Board , Representative Body and employees of Rochdale Boroughwide Housing ("RBH") are fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act"), which came into force on the 1st March 2000.

1.2 All public and private organisations are legally obliged to protect any personal information they hold and the Act is intended to promote a culture of openness and accountability by providing people with rights of access to all types of recorded information held by them

1.3 This document is a policy statement outlining our commitment and approach to data protection. RBH will therefore follow procedures that aim to ensure that all employees, Representative Body members, Board members, contractors, consultants and partners of RBH who have access to any personal data held by or on behalf of RBH, are fully aware of and abide by their duties and responsibilities under the Act.

## 2. Statement of Policy

2.1 In order to operate efficiently, RBH has to collect and use information about people with whom it works. These may include tenants and residents, the general public, clients, customers, suppliers, current, past and prospective employees, In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

2.2 RBH regards the lawful and correct treatment of personal information as fundamental to its successful operations and to maintaining confidence between RBH and those with whom it carries out business. RBH will ensure that it treats personal information lawfully and correctly. To this end RBH fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

## 3. What is Data Protection?

3.1 The Data Protection Act legally protects personal data on living individuals (Data Subjects); regardless of how the information is collected. Any organisation collecting and processing data must comply with the eight Data Protection Principles. RBH collects and controls such data in order to allow it to deliver housing management and other services that are appropriate to the needs of its tenants and residents.

This could include information about:

- people applying for a tenancy;
- repairs or refurbishment of the property;
- complaints about tenants, and;
- details of evictions or prosecutions.

### Data Protection and Email

3.2 Personal data includes any personal information stored in email messages and potentially, email addresses also. Employees must therefore comply with this Policy in relation to any personal data which is sent, received or stored in the form of an email.

### Data Protection and the Internet

3.3 The provisions of the Data Protection Act apply equally to processing on the World Wide Web as they do to processing on all other information systems. When personal data is submitted to RBH via the website the following information must be supplied to the Data Subject:

- The purpose for which the data is collected.
- The description of the organisations or individuals to whom the data might be disclosed.

## 4. The Principles of Data Protection

4.1 The Act places a legal obligation on all organisations to process personal data in accordance with ***Eight Principles*** of Data Protection. These Principles are legally enforceable.

4.2 The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure, that is appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.

## 5. Personal and "Sensitive" Personal Data

5.1 The Act provides conditions for the processing of any personal data. It also makes a distinction between ***"personal data" and "sensitive personal data"***. People may feel other data is sensitive but for the purposes of the act the following definitions apply:

5.2 ***Personal data*** is data consisting of information which relates to a living individual who can be identified from that data or from other information which is in the possession of, or is likely to come into the possession of RBH ("the Data Controller") and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller, or any other person in respect of the individual".

5.3 ***Sensitive personal data*** is personal data consisting of information as to:

- the racial or ethnic origin of the data subject;
- their political opinions;
- their religious beliefs or other beliefs of a similar nature;
- whether they are a member of a trade union;
- their physical or mental health conditions;
- their sexual life;
- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings".

## 6. Handling of personal/sensitive information

6.1 RBH will ensure that personal and sensitive information is processed in accordance with its legal obligations through the following criteria and controls:

- Full observation of the conditions regarding the fair collection and use of personal information;

- By specifying the purpose for which information is used;

- The collection and processing of appropriate information only to the extent that it is needed in order to fulfil operational needs or to comply with any legal requirements;

- Data used will be of a suitable quality in accordance with the RBH Data Quality Strategy;

- Strict checks will be applied to determine the length of time information is held (see paragraph on retention periods);

- By enabling the rights of people about whom the information is held to be fully exercised under the Act including:
  - The right to be informed that processing is being undertaken;
  - The right of access to one's personal information;
  - The right to prevent processing in certain circumstances;
  - The right to correct, rectify, block or erase information regarded as wrong information;

- Through the nomination of the Risk Manager as the designated officer with specific overall responsibility for data protection in the organisation;

- That service users and employees are made aware of who to approach with enquiries about handling personal information through media such as the tenants handbook, induction workbook, website, intranet and briefing sessions;

- All Board members will be made fully aware of the contents of this policy and of their duties and responsibilities under the Act through the annual appraisal system;

- That everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice and receive the appropriate training and supervision;

- That queries about handling personal information are promptly and courteously dealt with;

- Procedures for handling personal information and their application will be regularly assessed and evaluated to ensure that they remain 'fit for purpose';

- Where there is a legitimate requirement to share data with a third party this will be specified in an appropriate written protocol, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

- It will be the responsibility of all employees within RBH to take necessary steps in order to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular that:

  - Paper files and other records or documents containing personal/sensitive data are kept in a secure environment. Where personal data is being used by employees outside the normal secure office environment the necessary safeguards will be put in place in accordance with the RBH Records Management policy;
  - Personal data held on computer and other information technology systems is protected by the use of secure passwords, which where possible have forced changes periodically;
  - Portable devices such as laptops will also be encrypted;
  - Individual passwords should be such that they are not easily compromised;

- All contractors, consultants and partners of RBH must:

  - Ensure that they and all of their employees, who have access to personal data held or processed for or on behalf of RBH, are fully trained and aware of their duties and responsibilities to abide by the requirements of the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between RBH and that individual, company, partner or firm;
  - Allow data protection audits by RBH of data held on its behalf (if requested);
  - Indemnify RBH against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

## 7. Subject Access Requests

7.1 The Act gives all individuals the right to make a request, in writing, to obtain a copy of any information that RBH holds about them on computer and in certain manual filing systems. They are also entitled to be given a description of the information, what RBH use it for, who it might be passed on to and any information RBH may have about the source of the information.

7.2 The right applies to anyone about whom RBH holds information. This could be current and former employees, current and former tenants and residents, service users, suppliers and contractors. If, therefore, RBH holds data on individuals and, if the subject of the data so requests, RBH is required to provide details of the data held as described above, together with an explanation of any technical terms used in the information.

7.3 To exercise this right, individuals must make a subject access request. All such requests should be directed to the Risk Manager immediately.
RBH is legally obliged to respond to requests within 40 calendar days. Failure to do so is a breach of the act and could lead to a complaint to the Information Commissioner.

### Fees

7.4 RBH will charge a fee of up to £10 for each subject access request in line with the regulation. The person making the subject access request will be advised of this charge at the time of their request.

## 8. Circumstances Where Personal Data May Not Be Released To An Individual

8.1 RBH will provide personal information upon the receipt of a Subject Access Request unless a specific exemption, or exemptions, apply under Part IV and Schedule 7 of the Act e.g. If disclosure of personal information is likely to prejudice an investigation into the behaviour or activities of the person making the Subject Access Request or if it is in connection with eviction proceedings.

## 9. References to Other Individuals

9.1 Where personal information contains details about other people (third parties), e.g., complaints made by other tenants or comments made by a member of employees, RBH will still endeavour to supply as much information as possible by editing references to, or by seeking the consent of the third party.
However, in considering providing such information RBH will and take into account any potential conflict between an individuals right of access under the Act and a third party individuals right to privacy or confidentiality.

## 10. Requests for Information from a Third Party

10.1 Third parties are not generally entitled to have access to personal data pertaining to RBH data subjects unless RBH as the data controller is satisfied as to the identity of the third party requesting it. A common example of this would be a law centre or Citizens Advice Bureau acting on behalf of a client. In such circumstances RBH will require a signed authority from the data subject authorising the third party to act on their behalf before the release of any personal data can be considered. Assuming this is provided, information can be released.

10.2 The Data Protection Act also allows exemption from the general non disclosure provisions relating to personal data in circumstances where it is necessary for the purposes of any legal or prospective legal proceedings or for the purposes of obtaining legal advice. All such requests from third parties without a signed authority should be directed to the Head of Legal and Compliance.

## 11. Employee Training

11.1 Appropriate training will be provided for all employees that use or have access to personal data in the workplace. What is deemed "appropriate" will be determined by the level of risk involved, that is the frequency with which employees handle personal data.

11.2 All new members of employees will receive information about the act as part of their induction process, commencing with the "Getting Started" Workplace Induction Workbook.

11.3 All employees will then undergo annual refresher training.

## 12. Information Security

12.1 Under the Data Protection Act, security measures apply not only to the security of computer hardware and storage media but also to source documents including manual records, printouts and oral disclosure.
Security measures are also applicable throughout the use and processing of Personal data, including the handling, transmission, disclosure and disposal of documents containing personal data.
All Managers are responsible for ensuring that adequate security arrangements for personal data exist within their relevant areas. Although this responsibility may be delegated, it is the role of Managers to ensure that employees are aware of their responsibilities with regard to Data Protection

12.2 For the purposes of this Policy, the following definitions apply:

***Information*** is considered to be any knowledge or data that has a value to RBH and which is collected, processed, stored, communicated or received. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation.

***Security*** is considered to be the protection of information against unauthorised disclosure, transfer, modification, retention or destruction, whether accidental or intentional.

12.3 Employees are considered to be all permanent, temporary, casual, sessional and seconded employees of RBH, Elected Members, contracted third parties working for RBH and external agencies working in partnership with RBH, whether working on RBH premises, from third party premises or from home.

### Security Principle

12.4 RBH depends on its IT infrastructure for the retrieval, sharing and dissemination of business critical data, and for the conduct of its business. Failure to adhere to adequate security standards could result in the alteration, theft, destruction or loss of ability to process the data. In addition, some of the data stored is of a confidential or sensitive nature. Should this data become compromised then RBH could face legal action for failing to protect it adequately as required by the Data Protection Act 1998. Such action would considerably damage RBH's credibility and incur significant legal costs including the imposition of unlimited fines.

12.5 Loss or damage of important business assets such as customer contact databases could also result in incorrect business decisions or the perpetration of fraud.

12.6 All users of RBH's information systems are responsible for the protection of the organisation's information assets, both computer hardware and data.

12.7 Employees must report any action that appears to contravene the information security policy, any breach of information security or any suspected weakness immediately to the Risk Team.

### User Authentication

12.8 All information systems require a unique user identification and password to be entered before access to the systems will be granted. All users who are issued with a user ID and password must comply with RBH's IT Security policy. In addition all systems should be password locked when not in use, or when away from your work station for any length of time to prevent unauthorised access being gained on your log in.

### E-mail

12.9 All users who are granted access to the corporate e-mail system by whatever means must comply with RBH's Acceptable use of IT policy. All users will be provided with a copy of the Acceptable use of IT policy.

### Software

12.10. Unauthorised copying or removal of RBH owned software or software licensed to RBH may be a criminal offence and can serve as grounds for prosecution as well as the application of RBH's disciplinary processes.

### Printing

12.11 Secure printing allows all users to send their documents to network printers and have the job printed only when they are physically standing in front of the printer and have entered their PIN thus avoiding documents being picked up by another user or being left uncollected. This will also cut down on waste as print jobs sent in error can be cancelled before they print out. Any unprinted jobs will be deleted overnight. All users will use this facility and any documents left found discarded at a printer will be considered a breach of data protection.

### Discipline

12.12 Any individual found deliberately contravening this Standard or caught jeopardising the security of information that is the property of RBH will be subject to the organisation's disciplinary procedure. In addition, in appropriate cases, individual employees may be subject separately to legal action by the relevant authorities, including the Information Commissioner.

## 13. Retention Periods

13.1 The act requires that personal data should not be kept any longer than is necessary and should be destroyed once it is no longer relevant for the purpose for which it was collected. However, the act does not specify how long a period different types of personal data should be kept.

13.2 In order to comply with the act RBH will review all data processed and the purpose for such processing and then consider, in relation to each type of data, how long it will be kept for the relevant purpose.

13.3 The specified periods are detailed in the RBH Records Management policy.

## 14. Surveillance Systems

14.1 This policy covers the use of a number of surveillance systems including

- CCTV systems
- Covert surveillance camera
- Noise monitoring Systems

14.2 The aim of any surveillance system is to keep our neighbourhoods and communal areas clean and safe. In our offices the system will be used to prevent and detect crime and to help ensure the safety of employees and visitors. We will work with partner agencies to prevent and tackle anti social behaviour in our neighbourhoods and also take a zero tolerance approach to any such instances.

14.3 Surveillance systems will only be used where it is deemed appropriate, where it has been identified that surveillance monitoring is the best way of capturing information to deal with the issue or to prevent further occurrences.

14.4 In operating surveillance systems we aim to:

- Promote the health, safety and security of residents, employees and other users of buildings, communal areas and open spaces in our neighbourhoods
- Promote early actions that would save further damage to individuals or properties (e.g. making safe / repairing broken windows).
- Assist in the prevention and detection of crime, anti social behaviour, public order offences and other legal enforcement issues and in any subsequent capture and prosecution of those found to be responsible for these actions.
- We will operate an "observation and retrieval" type surveillance system, which allows approved personnel to listen to Noise Monitoring audio files, view live CCTV footage (e.g. of an interview room where a colleague may be working alone with a member of the public) and retrieve archived footage. This will be kept on the system for a period of between 30-40 days, before being securely destroyed.

### CCTV

14.5 We will follow guidance and good practice produced by the Information Commissioners Office, and the British Standards Institute Closed Circuit Television (CCTV) relevant codes of practice.

14.6 Cameras will be clearly visible at all times with appropriate signage displayed unless a covert operation is taking place in which case the camera will be hidden.

14.7 We will carefully consider the location and design of all CCTV cameras to ensure they provide the right quality of images to meet the required aims.

14.8 We will not use CCTV systems for the purposes of recording sound, providing live streaming for use on the internet, or for commercial purposes.

### Noise Monitoring

14.9 We will install noise monitoring equipment in various locations to detect and determine the source of noise disturbance which will be reviewed within an identified time period.

### Covert Surveillance

14.10 We will ensure that covert surveillance is proportionate to what it seeks to achieve.

14.11 We will ensure that surveillance equipment is appropriate for the purpose including where it will be fitted and how long it will be in place.

### Operations

14.12 We will securely store all images captured by the CCTV systems and limit access to authorised employees only.

14.13 We will provide secure access to any central control rooms and limit access to authorised employees only.

14.14 We will ensure that all employees who work in Central Control Rooms or undertake mobile patrols associated with the operation of CCTV systems have valid Disclosure and Barring Service (DBS) checks.

### Data Security, Retention and Disposal

14.15 We will limit access to images captured by surveillance systems to authorised employees and use appropriate security measures to prevent external interception.

14.16 We will normally keep CCTV images and Noise Monitoring Recordings for between a minimum of 30 days and a maximum of 40 days dependent on the systems in place.

14.17 Where requested by the Police or other legal enforcement agencies, or where it has been identified that the recordings hold data relating to activities which could be deemed as criminal or which may give rise to a claim against RBH, we may then retain digital images or Noise Monitoring recordings for up to 3 years.

14.18 Where legal proceedings are then commenced we will retain the data the duration of the proceedings and for a further 3 years after the completion of the proceedings.

## 15. Implementation

15.1 RBH has appointed the Head of Legal and Compliance to have designated responsibility for Data Protection. This officer will be responsible for ensuring that the Policy is implemented and will also have overall responsibility for:

- The provision of cascaded data protection training, for employees within RBH;
- Dealing with Subject Access requests;
- Carrying out compliance checks throughout the society to ensure adherence with the Data Protection Act.
- Investigating any breach of data protection and implementing any necessary corrective and preventative action

## 16. Complaints

16.1 If a data subject feels that they have not been given all the information they asked for, that it is incorrect, or they are dissatisfied with how RBH have handled or processed personal data or the Subject Access Request they may complain to RBH through the Compliments, Comments and Complaints procedure or appeal to the Information Commissioner at the following address:

Information Commissioners Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF

Tel: 08456 306060
Web: www.ico.gov.uk

## 17. Notification to the Information Commissioner

17.1 The Information Commissioner maintains a public register of data controllers and the RBH group of companies are registered as such. The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

17.2 Following consultation with designated officers the Head of Legal and Compliance will review the entries of RBH in the public register of data controllers on an annual basis, prior to notifying the Information Commissioner of any changes to the register within 28 days.

## 18. Equality and Diversity

18.1 An Equality Impact Assessment relevance test has been carried out for this policy and the outcome was found not to warrant a full Equality Impact Assessment.

## 19. Links to Other RBH Strategies and Policies

- Records Management Policy
- Code of Conduct for Employees
- Code of Conduct for Board Members
- Code of Conduct for the representative Body
- Openness and Public Disclosure Policy
- Disciplinary and Grievance procedures
- Anti Fraud, Bribery and Money Laundering Policy
- Agile Working Strategy
- Flexible Working Policy
- Homeworking Guidance Document
- IT Security Policy
- Acceptable use of IT Policy

## 20. Monitoring and Review

20.1 All RBH policies and procedures are reviewed on a regular basis in order to ensure that they are 'fit for purpose' and comply with all relevant legislation and statutory regulations.

20.2 This policy, including any other related policies and procedures will be reviewed annually in order to ensure its continued appropriateness and formally reviewed and submitted to the appropriate 'approving body' every three years.

20.3 This policy will be monitored by the Risk Group and Audit Committee who will receive notification of all significant data security breaches.

# APPENDIX 1

## Glossary of Terms

| Term | Definition |
|---|---|
| **DATA CONTROLLER** | A person who (either alone or jointly or in common with other persons) determines the purposes and manner in which personal data is to be processed.<br><br>The term 'Data Controller' replaces the term 'Data User' which was used In the previous 1984 version of the Act.<br><br>Rochdale Boroughwide Housing Ltd is the Data Controller for the purposes of the 1998 Act. |
| **DATA PROCESSOR** | Means any person, other than an employee of the Data Controller who processes data on behalf of the Data Controller. |
| **DATA SUBJECT** | Means an individual who is the subject of personal data held by the Data Controller. |
| **DISCLOSURE** | Means disclosing the data to a third party either within or outside of Rochdale Boroughwide Housing. |
| **EXEMPTION** | The Act contains a number of exemptions from the Data Controller's rights and duties under the Act that are designed to accommodate special circumstances. Rochdale Boroughwide Housing must process personal data in accordance with the Act unless one of these exemptions applies.<br><br>The exemptions either allow for the disclosure of information where there would otherwise be a breach of the Act (e.g. disclosure of personal information to a third party) or allow information to be withheld that would otherwise need to be disclosed. |
| **PERSONAL DATA** | Means data that consists of information which relates to a living individual who can be identified from that data, or from other information in the possession of the Data Controller (Rochdale Boroughwide Housing) or any other person in respect of the individual. |
| **PROCESSING** | Means obtaining, recording or holding information or data or carrying out any operational activity in relation to that data. |

| | |
|---|---|
| **RECIPIENT** | Means any person to whom the data or information is disclosed, e.g. an agent or employee of Rochdale Boroughwide Housing, a Data Processor or their agents or employees.<br><br>It does **not** include any person to whom Rochdale Boroughwide Housing may be required by law to disclose information to, e.g. the Police. |
| **SENSITIVE PERSONAL DATA** | Means data that consists of information relating to:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or similar beliefs<br>• Whether an individual is a member of a trade union<br>• Physical or mental health conditions<br>• Sexual life<br>• Offences or alleged offences<br>• Any proceedings for offences or alleged offences |
| **SUBJECT ACCESS REQUEST (SAR)** | A written request from an individual requiring the Data Controller (Rochdale Boroughwide Housing) to tell them whether you are processing their personal data and, if so, to provide them with a copy and with certain other information. This may include requests for house files, diary sheets and payment details.<br><br>In most cases a valid Subject access request must be responded to within 40 calendar days of receiving it |

# APPENDIX 2

## Reporting Information Security Breaches

A consistent approach to dealing with all Information Security breaches must be maintained across RBH. Breaches must be analysed and the Head of Legal and Compliance must be consulted to establish when a security breach needs to be escalated to a Security Incident. There are specific requirements to notify certain incidents to a variety of external bodies and serious breaches need to be notified to the Information Commissioners Office.

Centralised notification and control is necessary to ensure that immediate attention and appropriate resources are utilised to control, eliminate and determine the root cause of events that could potentially disrupt the operation of RBH or compromise data or sensitive information.

Security breaches have the potential to quickly escalate and could spread and cause data loss across the organisation. All employees must understand, and be able to identify Security Breaches and they must be reported immediately.

**The person who has identified the breach must report it immediately via the Head of Legal and Compliance.**

If the breach or incident is deemed to be an immediate threat to the security or stability of the ICT infrastructure, RBH will take immediate action to isolate the problem. This could include disabling network or account access for persons or equipment without prior notice.

All communications with the media regarding a breach will be coordinated through RBH's Communications Team.

## What is a Security Breach?

An information security breach would be caused when there is a failure to meet the requirements of the Data Protection Act. This includes the:

- loss of equipment
- loss of data including paper records
- unlawful sharing of personal data
- sharing of excessive amounts of personal data

RBH are required to manage & report actual breaches and near misses such as those listed below.

| | |
|---|---|
| A laptop or Memory Stick containing personal data is lost or stolen | A fax containing sensitive information is sent to the wrong number |
| Paper records are lost or stolen (vehicle theft, burglary, left on the bus) | An email is sent with files attached containing personal data to the wrong email address (internally or externally) |
| Personal data is transferred electronically outside the workplace and is not encrypted or sent securely. | Personal data shared legitimately with a 3rd party is lost, stolen or used inappropriately. |
| Password Sharing | Breaches of Building Security |
| Paper records containing personal data are left unsecured (on a desk, at the printer) | An employee uses personal data for a personal rather than a work related reason. |
| Too much personal information is shared (internally or externally) to get the job done | |

## Management of Information Security Breaches

Any breaches will be considered jointly by the Legal and Compliance Team and Human Resources. Dependent upon the seriousness of the allegations and the outcome of investigations employees should be aware that this may result in disciplinary action being taken which may have serious consequences for an employee's continued employment.

All breaches will be reported to the Head of Legal and Compliance for an initial assessment. Loss of equipment including mobile phones & laptops will also be reported to the IT Team immediately so they can suspend any further use of this equipment.

### Process

The incident management process will incorporate 4 key steps – Initial Reporting, Managing the Incident, Investigating, Final Reporting.

The Head of Legal and Compliance will undertake an initial assessment of the breach and oversee any subsequent investigation.

Other resources may also be identified to support the investigation e.g. line manager, Head of Service, IT, Internal Audit. Where the incident may lead to significant negative publicity and/or impact on delivery of day to day services the Incident Management team may also form. The investigation process will cover the following:

- Identification of the incident, analysis to ascertain its cause and any vulnerabilities it exploited.
- Limiting or restricting further impact of the incident.
- Tactics for containing the incident.
- Corrective action to repair and prevent reoccurrence.
- Communication across the society to those affected.

The Security Breach Notification Form needs to be completed for all breaches and near misses.

## Collection of Evidence

If an incident requires information to be collected for an investigation, strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care and be carefully documented.

## Risk Assessment

The incident should be risk assessed using the **Categorising Serious Incidents Requiring Investigation (SIRIs) process** at Appendix 3. This assessment includes the number of individuals affected, potential reputational damage, media interest and potential litigation. If the impact is 2 or greater, it must be immediately escalated to the Incident Management Team and reported to the ICO.

## Learning from Information Security Breaches

Key components should be extracted from the Security Breach Notification Form to learn from incidents, improve the response process and prioritise activities to improve compliance and reduce the recurrence of regular incidents. Any changes to the process made as a result of the Post Incident Review must be formally noted.

This information will be collated on a breach log which will be reviewed on a regular basis by the Legal and Compliance Team and any patterns or trends identified.

# APPENDIX 3

## Categorising Serious Incidents Requiring Investigation (SIRIs)

The SIRI category is determined by the context, scale and sensitivity. Every incident can be categorised as either level:

1. Confirmed SIRI but no need to report to ICO, and other relevant bodies.
2. Confirmed SIRI that must be reported to ICO, and other relevant bodies.

A further category of SIRI is also possible and should be used where it is determined that it was a near miss or the incident is found to have been mistakenly reported:

0. Near miss/reported in error

Where an SIRI has found not to have occurred or severity is reduced due to fortunate events which were not part of pre-planned controls this should be recorded as a "near miss" to enable lessons learned activities to take place and appropriate recording of the event.

**The following process should be followed to categorise an IG SIRI**

### Step 1

**Establish the scale of the incident. If this is not known it will be necessary to estimate the maximum potential scale point. Baseline Scale**

| Score | Description |
|---|---|
| 0 | Information about less than 10 individuals |
| 1 | Information about 11-50 individuals |
| 1 | Information about 51-100 individuals |
| 2 | Information about 101-300 individuals |
| 2 | Information about 301 – 500 individuals |
| 2 | Information about 501 – 1,000 individuals |
| 3 | Information about 1,001 – 5,000 individuals |
| 3 | Information about 5,001 – 10,000 individuals |
| 3 | Information about 10,001 – 100,000 individuals |
| 3 | Information about 100,001 + individuals |

## Step 2

Identify which sensitivity characteristics may apply and adjust the baseline scale point accordingly.

Sensitivity Factors

Low: For each of the following factors reduce the baseline score by 1

-1 for each
No sensitive data at risk
Limited demographic data at risk e.g. address not included, name not included
Security controls/difficulty to access data partially mitigates risk

Medium: The following factors have no effect on baseline score

Basic demographic data at risk e.g. equivalent to telephone directory

High: For each of the following factors increase the baseline score by 1

+1 for each
Detailed information at risk e.g. case/file notes
Particularly sensitive information at risk e.g. HIV, STD, Mental Health, Children
One or more previous incidents of a similar type in past 12 months
Failure to securely encrypt mobile technology or other obvious security failing
Celebrity involved or other newsworthy aspects or media interest
A complaint has been made to the Information Commissioner
Individuals affected are likely to suffer significant distress or embarrassment
Individuals affected have been placed at risk of physical harm
Individuals affected may suffer significant detriment e.g. financial loss
Incident has incurred or risked incurring an untoward incident

Step 3: Where adjusted score indicates that the incident is level 2, the incident will be reported to the ICO

| Final; Score | Level of SIRI |
|---|---|
| 1 or less | IG SIRI not reportable |
| 2 or more | IG SIRI Reportable |