	<b>POLICY</b>	RBS-HR 03E/05.18 - VB Page 1 of 2
	<b>DATA PROTECTION BREACH POLICY &amp; PROCEDURE</b>	

**POLICY STATEMENT**

The Company is committed to handling personal data in line with best practice and as such this Policy details the procedures to use when dealing with and responding to data protection breaches. This is to ensure that incidents are responded to promptly, risks are minimised, learnings identified and remedial actions are implemented.

This document has been designed to help and encourage all employees to achieve and maintain expected standards of conduct. It applies to all employees and anyone else working for the Company, and its aim is to ensure consistent and responsible practice.

This document does not form part of your Contractual Terms and Conditions of employment and the Company may at any time amend it without consultation or prior notice.

These procedures apply to all staff, suppliers, contractors, agency workers, volunteers, clients or anyone else who may handle or have an interest in personal data on behalf of the organisation.

**PURPOSE**

The purpose of an incident response is to ensure that:

- Data breach events are detected, reported, categorised and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of disclosure
- Mitigation improvements are made is put in place to prevent recurrence
- Serious breaches can be reported to the Information Commissioner
- Lessons learnt are communicated to the organisation as appropriate and can work to prevent future incidents.

**DATA PROTECTION BREACHES**

A data protection breach occurs when personal data (which includes any information that allows an individual to be identified), is processed without authorisation, and which may result in its security being compromised. For the purposes of this policy, data protection breaches include both confirmed and suspected breaches.

This procedure is concerned with the management of such data protection breaches, which involves the detection and reporting of breaches as well as learning from the breach and implementing appropriate remedial actions.

Most commonly, data protection breaches occur as a result of human error, theft, unauthorised access, equipment failure, hacking or loss

Examples of common incidents are

Type	Example
Technical	Data Corruption Malware Corrupt Code Hacking
Physical	Unescorted visitors in secure areas Break-ins to sites Thefts from secure sites Theft from unsecured vehicles/premises Loss in transit/post Loss/ Misplacing memory stick/flash drive confidential papers left on public transport
Other	Data Input errors Non-secure disposal of hardware or paperwork Unauthorised disclosures (including verbal)


When a data protection breach has been discovered, whatever the reason for the breach, the following procedure should be implemented

**DISCOVERY**

All staff are responsible for data protection and should be alert to any actual, suspected, threatened or potential data protection breaches. As soon as a data protection breach has been discovered, where possible, a Data Protection Breach Reporting Form should be completed to the fullest extent possible at that time, which provides full details concerning the breach. This form should then be passed to the Operations Director, as soon as possible and in any event within 2 hours of the discovery of the breach. If you need help completing the form, or are unable to complete the form, then any delay should be avoided and instead the matter should be reported immediately, either verbally or using electronic means, such as email.

Once a data protection breach has been reported, an initial assessment will be made concerning the content, quality of data involved and the potential impact and risk of the breach.

This is achieved by interviewing the key personnel involved in the breach and their line managers and collecting as much information as possible to determine how the breach occurred, what actions have been taken, whether outside agencies are involved and whether the data subjects have been notified

	<b>POLICY</b>	RBS-HR 03E/05.18 - VB Page 2 of 2
	<b>DATA PROTECTION BREACH POLICY &amp; PROCEDURE</b>	

Not all data protection breaches will result in formal ICO Reporting action. Some will be false alarms or “near miss” events that do not cause immediate harm to individuals or the organisation. These should still be reported, as analysis of these instances will provide valuable process feedback and opportunity for continual improvement.

### REPORTING

Following a discovery of a breach and the receipt of such a report, consideration will be made regarding whether the matter needs to be reported to the Information Commissioner’s Office (ICO) and whether individuals who are potentially affected need to be informed.

Current legislation states that any data protection breaches (irrespective of their severity) should be reported to the ICO as soon as possible and no later than 72 hours after their discovery, unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned.

In addition to this, the individuals affected by the breach should be informed if the breach is likely to pose a high risk to them. The individuals should be informed of the nature of the data breach and the steps that you are taking to protect their data.

The incident should also be logged in the Data Protection Breach Register.

### CONTAINMENT AND RECOVERY

As soon as possible after the discovery of an actual or suspected data protection breach, consideration should be given to: -

- whether the breach has been contained as far as possible and whether any further steps can be taken to contain the data from further loss;

- whether any steps can be taken to mitigate the impact and risk of the loss;
- whether anything can be done to recover the data.

### INVESTIGATION

Following the initial discovery/reporting of an incident, an investigation should be initiated to understand the full facts regarding the data protection breach. The extent of the investigation will be a matter for the Company to decide and may simply involve the collation of documents, or may be involve interviewing staff involved in the breach, collecting witness statements, etc.

### REMEDIAL ACTIONS

Once the full facts have been ascertained, and the investigation has been concluded, consideration will be given to the learnings from the breach and most importantly, what remedial actions the organisation needs to take to prevent a recurrence of the incident, this may include any appropriate disciplinary action for individuals implicated in the breach.

Actions should be documented on an action plan, which is reviewed on a regular basis thereafter to ensure that the actions have been carried out.

During and/or at the end of the completion of the investigation the Data Protection Breach Reporting Form and the Data Protection Breach Register will be updated to ensure that all the details of the events have been properly documented.

Any employees who act in breach of this policy or who do not implement it, may be subject to formal disciplinary proceedings, which may involve dismissal depending on the relevant circumstances.