Policy document control box	
Policy title	**Data Breach Policy**
Policy owner	Brooke Hornby Operations Lead
Version	1.00
Approving body	
Date of meeting when version approved	November 2023
Date of next review	November 2024

Policy contents:

Contents

Data Breach Policy

1. Introduction

This policy is designed to ensure that all employees, trustees and volunteers can identify data breaches and meet the requirements of Data Protection Legislation in the handling of a personal data breach (henceforth “personal data breach” or “data breach”).

Data Protection Legislation means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

2. Definitions

- Any reference to “Article” or “Articles” is a reference to an Article or Articles of the “UK GDPR”
- The terms ‘personal data’, ‘data subject’, ‘processing’, ‘pseudonymisation’, ‘controller’, ‘processor’, ‘recipient’, ‘third party’, ‘consent’, ‘personal data breach’, have the meanings set out in Article 4 of the UK GDPR
- “Security incident” means an incident in which the security of personal data may have been compromised but no risk is identified in respect of the rights and freedoms of data subjects. Security incident in the context of this policy may also be used to define an event or action which may compromise the confidentiality, integrity or availability of systems or data, where such event or action does not presently amount to a data breach.
- The term DPO refers to the RBET Data Protection Officer.

3. What is a Data Breach?

A personal data breach is defined within the Data Protection Legislation as “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”.

The notification requirements associated with data breaches rest on the level of risk to the rights and freedoms of data subjects arising from the breach. Unless a personal data breach is unlikely to result in a risk to the rights and freedoms of the concerned data subjects, it is to be reported to the ICO or relevant supervisory authority. Where such data breaches are likely to result in a high risk to the rights and freedoms of the concerned data subjects, the affected data subjects are to be informed in addition to the supervisory authority.

Data Protection Legislation further stipulates that where notification of the supervisory authority is required, this should take place within 72 hours of the controller becoming aware of the personal data breach. In the case of breaches which pose a high risk to data subjects, the additional requirement to notify data subjects must be done as soon as possible and without undue delay.

In light of these requirements, this policy focuses on the responsibilities of all employees, agents and contractors in internally reporting incidents and breaches and the external notification requirements.

4. Responsible Persons

The Red Balloon Educational Trust Trustees have overall responsibility for ensuring that any privacy risks are managed.

All users of information assets across the organisation should familiarise themselves with this procedure, be aware of privacy risks and be vigilant in order to ensure breaches are identified, reported and managed in a timely manner.
All staff are responsible for reporting mistakes, suspected or actual data breaches at any given time. They must report all incidents, including those resulting from human error and those with unidentified or unknown affected data subjects as soon as detected.

Support will be provided to ensure everyone has access to the appropriate skills and training to carry out their role effectively. However gross negligence and intentional violations (including not reporting incidents/mistakes) are taken seriously and could lead to disciplinary action.

5. Breach Response Process

a) Identify the breach

Personal data breaches could include:

- access by an unauthorised third party
- human error affected personal data
- sending personal data to an unauthorised recipient;
- network intrusions
- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- alteration of personal data without permission;
- loss of availability of personal data.

b) Report the Breach

When reporting a security incident or personal data breach, suspected or actual, the reporter is obliged to disclose all information within their knowledge using the **Breach Report Form** annexed to this Policy (Annex 1).

This must be submitted to the Red Balloon Educational Trust DPO immediately.

The Red Balloon Educational Trust DPO will analyse the form, update the Data Breach Register, investigate the breach and ascertain whether any immediate corrective, containment or escalation actions are required.

c) Investigate the Breach

Red Balloon Educational Trust aims to complete a preliminary investigation of all reported incidents without undue delay, with an aim to establish its awareness of a personal data breach within the **first 24 hours** of internal detection.

From the point of detection, there are **72 hours** within which to identify whether there is a risk to the concerned data subjects and where there is a risk, notification to the supervisory authority should take place.

During the investigation, Red Balloon Educational Trust will aim to establish the following:

- the facts of the security incident
- the data or records concerned
- the value and sensitivity of the data or records concerned
- the type of breach suspected (confidentiality, integrity, availability)
- the number and identity of affected data subjects
- identify and assess the ongoing risks (by carrying out a **Root Cause Analysis**) that may be associated with the breach. In particular, an assessment of;

(a) potential adverse consequences for individuals,

(b) their likelihood, extent and seriousness.

Determining the level of risk will help define actions in attempting to mitigate those risks and determine any onward notification responsibilities.

- the measures required to contain the impact of the breach.

d) Notify the Supervisory Authority

All personal data breaches which pose a risk to the rights and freedoms of data subjects must be reported to the Information Commission's Office (ICO) within 72 hours of becoming aware of a relevant breach.

Red Balloon Educational Trust aims to ensure all such notifications are made within 72 hours of becoming aware of the personal data breach.

All notifications to the ICO must be made by the Red Balloon Educational Trust DPO or an authorised individual in their absence and will be made using the breach notification form provided by the ICO.

e) Notify the affected Data Subjects

Where a high risk to the rights and freedoms of data subjects is established in the Risk Assessment, Red Balloon Educational Trust will inform data subjects of the personal data breach as soon as possible and without undue delay.

Communication to data subjects should include:

- the nature of the breach
- the name and contact details of the DPO or other contact person

- the likely consequence of the breach
- the measures taken or proposed to be taken by the controller to address the breach
- any recommended steps to be taken by the data subjects themselves e.g. changing passwords.

Red Balloon Educational Trust aims to notify data subjects of relevant personal data breaches directly unless it is impossible to do so, or it would involve a disproportionate effort, in which case the breach may be communicated by way of a public statement. All such communications must be authorised by an executive employee.

f) Notify Others

Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.

These could be police, other regulatory or supervisory authorities, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

This list is not exhaustive.

6. Accountability

All security incidents reported will be documented regardless of whether the breach was notifiable to the ICO. Red Balloon Educational Trust will maintain a Data Breach register containing all incidents which occur within the organisation.

7. Evaluation

The Red Balloon Educational Trust DPO will evaluate the effectiveness of the response to the breach to learn and apply any lessons or remedies or recommendations in the light of findings or experience across the organisation.

8. Annex 1

Please complete this digital form if you have detected or been advised of a data breach and upload any relevant attachments to the submission.

RBET Data Breach Report Form - Internal Use

It is imperative that you complete this form immediately upon detection of any potential breach.

Once completed, this form will automatically be sent to dpo@rbet.ac and your line manager. Where possible, please advise your line manager that you have completed this form due to a suspected breach immediately.

For reference, below is a demonstration of the digital Red Balloon Educational Trust Breach Report Form.

Incident / breach details	
Name of person reporting incident:	
Contact details of person reporting incident:	
Date(s) incident took place:	
Date you detected the incident:	
Place of incident:	
Brief description of how you became aware of the incident:	
Brief description of the incident including details of the data, records or systems believed to be affected:	
Approximate number of affected data subjects, if known:	
Approximate number of affected records, if known:	
Any actions taken in response to the incident:	