





## Data Breach Policy

<b>Policy Date:</b>	20 <sup>th</sup> September, 2021	<b>Version: 1.1</b>		
<b>Policy Review Date:</b>	September 2024	Headteacher Debra Bailey	Signed 	Insert Date 20/09/21
<b>Ratified by Governing Body:</b>				
Sue Welford (Chair of Governors)		Insert Signature 	Insert Date 20/09/21	

## Contents

Introduction.....	3
Scope .....	3
Purpose.....	3
Definitions.....	4
Examples of incidents which must be reported to the school DPO .....	4
Responsibilities .....	4
Reporting a data breach .....	5
Investigating a data breach.....	5
Assessing a data breach .....	5
Notifying a breach to the ICO.....	6
Notifying data subjects.....	6
Review and planning .....	7
Disciplinary procedure .....	7

## **Introduction**

The Information Commissioner's Office (ICO) describes a personal data breach as "a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just losing personal data."

Data security breaches are increasingly common occurrences, whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. Rushey Mead Primary School (RMPS) needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

In order to comply with the UK General Data Protection Regulation (GDPR), Rushey Mead Primary School (RMPS), as an organisation which processes personal data, must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Where such measures fail, this policy must be followed.

## **Scope**

This document sets out RMPS's policy for dealing with data breaches that may involve personal data. It applies to any security incident relating to personal data or the systems on which it is held and includes accidental loss, unauthorised access to, theft and destruction of personal data (referred to in this policy as an *incident*).

## **Purpose**

The purpose of this document is to specify actions to be taken in the event of a data breach that may involve personal data.

The approach outlined in this document aims to minimise the adverse impact of any breach of personal data that is held by RMPS. The actions, taken in a timely and comprehensive manner, will minimise damage sustained by the breach. By reviewing and learning from experience, the risk of incidents re-occurring is reduced. It applies to all personal data available to RMPS, irrespective of the source of the data or the media upon which it is held.

The implementation of this policy will:

- Facilitate a fast response to incidents in order to contain or minimise the impact on data subjects affected by the breach.
- Minimise RMPS's exposure to financial loss, reputational damage or legislative compliance.
- Clarify the responsibilities of those involved in managing and reporting personal data incidents.
- Provide support to those who are affected by the incident, both the data subjects and those staff directly involved.
- Provide information regarding the causes of the data breaches so that improvements can be made to mitigate the risk of a further occurrence. Reporting incidents should be viewed positively and is to be encouraged, as they often result in improved services or provide clarification of procedures which have been missing.

## Definitions

### **Personal data**

Any information relating to an identifiable living person ('data subject').

### **Special category data (sensitive personal data)**

The UK GDPR defines special category data as:

- Personal data revealing racial or ethnic origin;
- Personal data revealing political opinions;
- Personal data revealing religious or philosophical beliefs;
- Personal data revealing trade union membership;
- Genetic data;
- Biometric data (where used for identification purposes);
- Data concerning health;
- Data concerning a person's sex life; and
- Data concerning a person's sexual orientation.

Criminal convictions or offences (alleged or proven) are not technically defined as special category personal data, but are afforded similar protections.

### **Examples of incidents which must be reported to the school DPO**

Examples of potential breaches of data security which must be reported to the school Data Protection Officer (DPO) include:

- Phishing attempts in emails, for example emails that appear to be from a legitimate sender but contains malicious links.
- Sending non-essential personal data to otherwise valid recipients.
- Failure of access controls, such as incorrect allocation of permission or password sharing, which results in inappropriate or unlawful access to personal data.
- Loss or theft of paper containing personal data.
- Personal data received in error.
- Unnecessary publication of personal data on a website.
- Loss or theft of any RMPS owned data storage device, regardless of the data it contains, e.g. laptop, PC, USB, mobile phone, iPad or other tablet, removable hard drive, smart phone or other portable devices, or paper containing similar information.
- Unforeseen circumstances which affect the school's storage and use of personal data, such as a fire or flood.
- Instances where information is obtained by deceiving the holder of the information.
- Unauthorised disclosure of sensitive/personal data.

Loss or theft of any privately-owned devices should also be reported if they contain personal data related to RMPS activities.

### **Responsibilities**

Information users: All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

## Senior Management Team

The Senior Management Team is responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

## Reporting a data breach

Any individual who has access to, uses or manages school information, including staff, governors and data processors, must report a breach (or potential breach) that they have discovered or caused to the school DPO by sending an email to [wwest@rusheymead-pri.leicester.sch.uk](mailto:wwest@rusheymead-pri.leicester.sch.uk). RMPS will then liaise with the school's DPO consultants, BLS Stay Compliant Limited. Breaches should be reported as soon as possible after they have been discovered or the school notified of the incident.

The DPO will:

- Investigate the report and determine whether a data breach has occurred. If a breach has occurred, the actions to be taken will vary depending on the types of data and number of data subjects involved.
- Establish whether there is anything that can be done to recover any losses and limit the potential damage of the incident.
- Determine who, if anyone, may need to be notified of the breach, including informing the ICO and police, where appropriate.
- Determine the suitable course of action to be taken to ensure a resolution to the incident.

## Investigating a data breach

The management response to any reported data security breach will involve the following four elements:

- A. Containment and Recovery
- B. Assessment of Risks
- C. Consideration of Further Notification
- D. Evaluation and Response

All members of staff and governors must cooperate with the investigation, including allowing access to their devices and answering questions if they are required to so by the DPO. Staff under the direction of the DPO will make all reasonable efforts to contain and minimise the impact of a breach using external advice when required (e.g. from IT provider). If the DPO finds that a breach has occurred, or is likely to occur, then the DPO will alert the Headteacher and Chair of Governors.

## Assessing a data breach

Whilst investigating the incident, the DPO will assess:

- The type and level of personal data involved.
- If the incident is likely to result in a high risk of adversely affecting individuals' rights and freedoms.
- What security protections are in place (e.g. encrypted documents etc.).
- What has happened to the data (e.g. has it been lost, stolen or unlawfully accessed?).
- The sensitivity of the data (e.g. is the data special category?).
- Whether the data could be put to any illegal or inappropriate use.

- The data subjects involved, including the number and the potential effects on those individuals.
- Whether there are wider consequences to the breach.

The DPO will assess the potential consequences based on the severity of the incident and how likely the consequences are to happen before and after the implementation of steps to mitigate such consequences.

The DPO will advise the Headteacher whether the breach must be reported to the ICO, and the individuals affected (data subjects).

The DPO will document the decisions made (including to report or not) in case it is challenged at a later date by the ICO and / or an individual affected by the breach. Documented decisions are stored on the school's secure server, which can be accessed by the Business Manager.

### **Notifying a breach to the ICO**

Not all breaches need to be notified to the ICO, but if the breach is likely to cause a risk to the rights and freedoms of the individuals who are affected, then the incident must be reported to the ICO within 72 hours of the school becoming aware of the breach.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. The DPO must still notify the ICO of the breach when they become aware of it and submit further information as soon as possible.

Where a breach is considered to be notifiable, the DPO will report the incident to the ICO via the 'report a breach' page on the ICO's website: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>.

When reporting a breach, the UK GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

### **Notifying data subjects**

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR requires the school to inform those concerned directly and without undue delay.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, then the requirement to inform the individuals is higher than for notifying the ICO. The DPO will assess the severity of the potential or actual impact on the individuals as a result of a breach and, where appropriate, will advise the school to notify those individuals at 'high risk' promptly so that they can take their own steps to protect themselves from the effect of the breach.

If the school is required to communicate with the individuals affected by the breach, they must describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of the data protection officer, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

### **Review and planning**

The Business Manager will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Incident circumstances.
- Cause, where known.
- Actual and potential effects.
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

The DPO and Headteacher will meet as soon as possible after the incident to review what happened and any lessons to be learned to prevent future similar breaches.

The DPO, Business Manager and Headteacher will meet at least annually to assess any recorded data breaches and identify any trends or patterns requiring actions by the school to reduce risks of future breaches.

### **Disciplinary procedure**

Staff members and governors who act in breach of this policy may be subject to disciplinary procedures or other appropriate sanctions.