Rickleton Primary School

Data Breach

Dates of previous revisions: November 2024
Latest revision: November 2025

Approved by Governors: November 2025

To be reviewed: November 2026

Review Date	Changes made	Ratification Date by Governing Body
November 2020	No changes	December 2020
November 2021	No changes	November 2021
November 2022	No changes necessary at present after referring to DPO	Nov 2022
November 2023	As above	Nov 23
November 2024	No changes necessary after referring to DPO	Nov 24
November 2025	No changes necessary after referring to DPO	Nov 25

Data Breach Policy

Rickleton Primary School

1.0 **Introduction**

1.1 Rickleton Primary School holds processes and shares a large amount of personal data, a valuable asset that needs to be protected.

1.2 Every care is taken to protection personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individuals, reputational damage. Detrimental effect on service provisions, legislative non- compliance, and /or financial costs.

2.0 **Purpose**

2.1 Rickleton Primary School is obliged under the Data protection Act and the General Data Protection Regulation to

2.2 Have in place a framework designed to ensure security of all personal data during its lifecycle, including clear lines of responsibility**.**

2.3 This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the school/academy.

3.0 **Scope**

3.1 This policy relates to all personal and special category data held by the school regardless of format

3.2 This policy applies to all staff and pupils and contractors at the school. This includes teaching students, temporary, casual, agency staff, suppliers and data processors working for or on behalf of the school.

3.3 The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what remedial action is necessary to secure personal data and prevent further breaches.

4.0 Definition/types of breach

4.1 For the purposes of this policy, data security breaches include both confirmed and suspected incidents.

4.2 An incident in the context of this policy is an event which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the school's/academy's information assets and/or reputation.

4.3 An incident includes but is not restricted to, the following :-

- Loss or theft of confidential or special category data or equipment on which such data is stored (e.g loss of a laptop, memory stick, I Pad/Tablet or paper record.
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed successful) to gain unauthorised access to information or I.T systems
- Unauthorised disclosure of special category/ confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire of flood
- Human Error
- Blagging offences where information is obtained by deceiving the organisation who holds it.

5.0 Reporting an incident

5.1 Any individual who accesses, uses or manages the School's data is responsible for reporting the data breach and information security incidents immediately to **gdpr@rickletonprimary.co.uk**

5.2 The school will inform the Data Protection Officer

5.3 If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable. N.b the school only has 72 hours to report a breach to the Information Commissioner.

5.4 The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many people are involved. An incident reporting form should be completed as part of the reporting process. See Appendix 1

6.0 Containment and recovery

6.1 The Data Protection Officer will firstly determine if the breach is still occurring> if so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2 An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach, in some cases it could be the DPO)

6.3 The Lead Investigation Officer (LIO) will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

6.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the Police , where appropriate.

6.5 The LIO, in liaison with the relevant officers determine the suitable course of action to be taken to ensure a resolution to the incident.

7.0 Investigation and Risk Assessment

7.1 An investigation will be undertaken by the LIO immediately and where possible within 24 hours of the breach being discovered/reported.

7.2 The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse effects for individuals, how serious or substantial those are and how likely they are to occur.

7.3 The investigation will need to take into account the following:-

- The type of data involved
- It's sensitivity
- The protection in place (e.g encryption)
- What's happened to the data, has it been lost or stolen
- Whether the data could be put to illegal or inappropriate use
- Who the individuals are, the number affected and the potential effects on those data subjects
- Whether there are wider consequences to the breach

8.0 Notification

8.1 The LIO and/or the DPO, in consultation with the Headteacher, will; determine whether the breach needs to be reported to the Information Commissioner.

8.2 Every incident will be assessed on a case by case basis; however , the following will need to be considered:-

- Whether there are any legal/contractual notification requirements
- Whether notification would assist the individual affected – could they act on information to mitigate the risks
- Whether notification would help prevent the unauthorised or unlawful use of personal data
- Would notification help the school meet its obligations under the principle
- Whether this breach constitutes a high risk to individuals and therefore needs to be reported to the ICO

8.3 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the school for further information or to ask questions about what has occurred.

8.4 The LIO and/or the DPO must consider notifying third parties such as the Police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

8.5 The LIO and or DPO will consider whether any press release may be required.

8.6 All actions will be recorded by the LIO and DPO.

9.0 Evaluation and response

9.1 Once the initial incident is contained , the DPO will carry out a full review of the causes of the breach, the effectiveness of the response and whether any changes to systems, policies or procedures should be undertaken.

9.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

9.3 The review will consider:-

- Where and how the personal data is held and where it is stored
- Where the biggest risks lie , and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches.

If you discover a data breach, please notify the Head Teacher or Business Manager immediately and report it via data.protection@sunderland.gov.uk

Report details:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Date of report:	
If there has been a delay in reporting this breach to the DPO, please explain why:	

Details of the Breach:	
What has happened? Tell us as much as you can about what happened, what went wrong and how it happened.	
How did you find out about the breach?	
When was the breach discovered? Please include date and time	

When did the breach happen? Please include date and time where possible	
Categories of personal data involved in the breach: Please list all categories of data that have been affected	*E.g.: name, address, bank details, UPN, SEN Information, Assessments etc*
Number of personal data records concerned?	
How many data subjects could be affected?	
Categories of data subject affected?	*E.g.: students (current and past), staff, volunteers*
Potential consequences of the breach: Please describe the possible impact on data subjects because of the breach. Please state if there has been any actual harm to the data subjects	
What is the likelihood that the data subjects will experience consequences because of the breach?	☐ Very Likely ☐ Likely ☐ Neutral ☐ Unlikely ☐ Very Unlikely ☐ Not yet known
Has the staff member involved in this breach received data protection training in the last two years? Include date if yes	

Action Taken:	
Describe the actions you have taken or proposed to take as a result of the breach: Include actions you have taken to fix the problem and to mitigate any adverse effects	

Date action taken or proposed to be taken:	

Cyber Incidents only:	
Has the confidentiality, integrity or availability of information systems been affected? Identify which if applicable	
What is the impact of this?	☐ **High** – have lost ability to provide critical services ☐ **Medium** – have lost ability to provide some critical ☐ **Low** – no loss of efficiency and can still provide all critical services ☐ **Not yet known**
Likely recovery time:	☐ **Complete** – recovery is fully complete ☐ **Regular** – you can predict recovery time with existing resources ☐ **Supplemented** – you can predict recovery time with additional resources ☐ **Extended** – you cannot predict recovery time and need extra resources ☐ **Not Recoverable** – recovery is not possible, e.g. backups can't be restored ☐ **Not yet known**

For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	
Incident number	**e.g. year/001** *Use Iken Ref when available*
Follow up action required/recommended:	

Notification to ICO advised?	**YES/NO** **If YES, notified on:** **Details:**
Notification to data subjects advised?	**YES/NO** **If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder advised?	**YES/NO** **If YES, notified on:** **Details:**
Notification to police advised?	**YES/NO** **If YES, notified on:** **Details:**