Data Breach Policy

Policy Code:	HR6A
Policy Start Date:	July 2024
Policy Review Date:	July 2027

Please read this policy in conjunction with the policies listed below:

- HR6 Data Protection Policy
- HR5 ICT Acceptable Use Policy
- HR12 Staff Disciplinary Policy
- HR33 Records Management Policy
- HR36 Complaints Policy
- ICT1 CCTV Policy
- ICT2 Online Safety (Staff) Policy
- SW5 Safeguarding and Child Protection Policy
- SW9 Parental Communications and Complaints Policy
- SW17 Safeguarding Adults Policy
- Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill

1 Policy Statement

1.1 The Trust holds a large amount of data/information, both in hard and soft copy. This includes personal or confidential information (about people), and also non-personal information which could be sensitive or commercial, for instance financial data, performance reviews and similar information.

1.2 Care should be taken to protect this type of data/information, to ensure that it is not changed (either accidentally or deliberately), lost, stolen or falls into the wrong hands; that its authenticity and integrity is maintained.

1.3 In the event of a breach, it is vital that appropriate action is taken to minimise (or potentially eliminate) associated risks.

1.4 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1.5 References to the Trust or Academy within this policy specifically include all primary, secondary and special academies within the Trust, as well as the Early Years setting at the Priory Witham Academy, Priory Apprenticeships and Lincolnshire SCITT.

1.6 This policy does not form part of any member of staff's contract of employment and it may be amended at any time.

2 Roles, Responsibilities and Implementation

2.1 The Pay, Performance and HR Committee has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. This committee delegates day-to-day responsibility for operating the policy and ensuring its maintenance and review to the Data Protection Officer.

2.2 Leaders and Managers have a specific responsibility to ensure the fair application of this policy and all employee are responsible for supporting colleagues and ensuring its success.

3 Aims

3.1 The Trust aims to ensure that all personal data collected about staff, pupils, parents/carers, governors, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Act 2018 (DPA 2018), as set out in the Data Protection Bill and UK-GDPR.

4 What is a breach?

4.1 A data breach is an incident in which any personal or special category data is compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Some examples include:

- accidental loss, or theft of equipment on which data is stored or of the paper copies;
- unauthorised access to data;
- human error such as emailing data by mistake;
- failure of equipment and hence data held on it;
- loss of data or equipment through fire or flood, for instance.
- hacking attack; and
- where information is obtained by deceiving a member of staff.

5 Reporting of the breach

5.1 Data security breaches should be reported immediately or as soon as a member of staff becomes aware of the breach. Academy staff should report a breach to their setting's Data Protection Lead (DPL) or, in their absence, the Trust's Data Protection Officer (DPO). Staff from the Central Services should report any breach to the Trust's DPO or, in their absence, the Federation Data Manager.

Contact details:
DPO@prioryacademies.co.uk / 01522 871370

5.2 The breach report should include full and accurate details of the incident, including who is reporting the incident, what type of data is involved, if the data relates to people, how many people are involved.

6 Investigation and Risk Assessment

6.1 The Data Protection Officer will instigate a response and an investigation will be started within 24 hours of the breach being discovered, where possible. Please see Appendix A for the Trust's Data Breach Procedure.

6.2 The investigation will establish the nature of the breach, the type of data involved, whether the data is personal data relating to individuals, and if so, who are the subjects and how many are involved.

6.3 The investigation will consider the extent of the sensitivity of the data, and perform an assessment of the potential or actual consequences of its loss, for instance whether harm could come to individuals or to the Trust.

7 Containment and Recovery

7.1 The Data Protection Officer will determine the appropriate course of action and the required resources needed to limit the impact of the breach. This might require isolating a compromised section of the network, alerting relevant staff or shutting down IT systems.

7.2 Appropriate steps will be taken to recover data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

7.3 Advice from relevant departments across the Trust may be sought.

8 Notifying data subjects

8.1 Where a breach has occurred, and there is a risk to people's rights and freedoms as a result of the breach, the Trust, where possible, will take steps to notify the affected data subjects as soon as possible.

8.2 Information will be provided to the data subjects about the breach, and any steps taken to contain it.

8.3 Data subjects will be informed if the breach is reported to the Information Commissioner's Office (ICO) (see Section 9), and will be kept updated in relation to the outcome of the breach report.

9 Reporting a breach to the Information Commissioner's Office (ICO)

9.1 Further to an assessment being carried out, as referenced in 6.3, if it is identified that there is a risk to people's rights and freedoms following the breach, then the Trust will report the breach to the ICO. If required, the Trust will seek advice from the ICO as to whether or not the breach is reportable.

9.2 In line with ICO guidance, the breach must be reported within 72 hours of the Trust becoming aware of the breach. In exceptional circumstances, where this timeframe is not adhered to, the reason for this will be explained in the report submitted to the ICO.

10 Review

10.1 Once the breach is contained, a thorough review of the event will be undertaken to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement or additional training.

10.2 Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible after consultation with the relevant staff.

10.3 If the data breach investigation finds that the breach is a result of a member of staff's action or there had been any unreasonable delay in the reporting of the breach this will lead to a disciplinary procedure. This will be dealt with through HR12 Staff Disciplinary Policy.

11 Policy Change

11.1 This policy may only be amended or withdrawn by the Priory Federation of Academies Trust.

The Priory Federation of Academies Trust

Data Breach Policy

This Policy has been approved by the Pay, Performance and HR Committee:

Signed…… Name..... Date:

Trustee

Signed…… Name..... Date:

Chief Executive Officer

Signed…… Name..... Date:

Designated Member of Staff

Please note that a signed copy of this agreement is available via Human Resources.

Appendix 1 – Data Breach Procedure