PENTREBANE PRIMARY SCHOOL DATA PROTECTION INCIDENTS POLICY AND PROCEDURE

(REVIEWED AND UPDATED MARCH 2026)

1 Introduction

1.1 Pentrebane Primary School is legally required under the Data Protection legislation to ensure the security and confidentiality of the information/data it processes on behalf of its clients and employees.

1.2 Sometimes a loss of data may occur because this information/data is accidentally disclosed to unauthorised persons or, lost due to a fire or flood or, stolen as result of a targeted attack or the theft of a mobile computer device.

2 Legislation

2.1 Pentrebane Primary School has an obligation to abide by all relevant legislation and European directives, including the:

The Data Protection Act 2018
The General Data Protection Regulation
Human Rights Act (1998)
Privacy and Electronic Communications Regulations (2003)
GDPR (2018)

3 Responsibilities

3.1 The Head teacher and Governing Body, supported by the Data Protection Officer maintains overall responsibility for ensuring compliance with this procedure, including coordinating and managing the response to any reported incident, documentation of all steps taken, evidence collection, and closing out the Event, including overseeing any recommendation/actions as a result of the breach.

3.2 All employees have a responsibility to be aware of potential Security Incidents as defined in this Policy and are required to report all incidents, both actual and suspected.

3.3 All Incidents must be reported to the Data Protection Officer via SchoolsInformationManagement@cardiff.gov.uk immediately, but no longer than 24 hours after which the incident was known. Where an incident occurs over a weekend, which is not classed as a working day, such incidents must be reported no later than 12 noon on the next working day.

3.4 Reporting should be via the Schools Data Protection Incident Report Form at Appendix 1 of this Policy. It should be emailed to SchoolsInformationManagement@cardiff.gov.uk

Head Teachers or Schools staff themselves must not investigate what appears to be an incident.

3.5 The Data Protection Officer may in appropriate cases authorise relevant officers to conduct such investigations. In such cases, reports into such incidents must be carried out immediately to ensure that any necessary action(s) is promptly taken with the final report issued to the Statutory Data Protection Officer

3.5 Technical staff and other relevant personnel are required to fully support the Data Protection Officer or staff as designated by the Data Protection Officer, in dealing with an Incident.

4 Data Protection Incidents

4.1 A Data Protection Incident is a situation where the School has lost control of the processing of data that contains personal and or confidential information which could result in distress/harm to the individuals (Data Subjects) whose data has been compromised or affect the commercial interests of third-party organisations. Further details, of types of data, is specified in the Schools Data Protection Policy & Procedure.

4.2 Examples of Data Protection incidents would include loss of paper-based records that contain personal/confidential information of third-party individuals, including citizens, businesses, employees, children

or parents; this also includes commercially sensitive information (including contracts). Other typical examples include loss of control of documents containing the above information sent to third party individuals or internally, this would include emails sent to incorrect recipients or to generic mailboxes, or faxes sent to the incorrect number, or loss of an asset such as laptops, storage devices, mobile phones etc.

4.3 Any complaints from a member of the public or an employee that they believe that their data may have been breached, or their rights of privacy have not been kept must be reported immediately to the Data Protection Officer via SchoolsInformationManagement@cardiff.gov.uk

4.4 Any individual who becomes aware of an actual, suspected or potential Data Protection Incident must complete the Data Protection Incident report form (see Appendix 1), forward it to SchoolsInformationManagement@cardiff.gov.uk AND report it immediately to the Head Teacher.

5 Management of Reported Incidents

5.1 The Data Protection Officer, on behalf of Head Teacher and Governing Body will log all incidents immediately and will log the progress of an investigation, including the collection and securing of any relevant evidence as the investigation progresses.

5.2 Any information gathered during the course of an investigation is treated as potential evidence in a disciplinary, criminal or civil action. If the likelihood of legal, civil or criminal action is established, the involvement of police and legal support will be enlisted at the earliest opportunity.

5.3 All evidence, in any format, will be retained securely by the Data Protection Officer, who will have sole responsibility for the authorising of access to other personnel as appropriate. All evidence will be retained for a period of seven years.

5.4 In the event of multiple 'incident' Reports the Data Protection Officer, will prioritise response according to the criticality of the data at risk, or the danger of further compromise to the data subjects. How incidents are assessed is set out in Appendix 3.

5.5 The Data Protection Officer is responsible for closing the incident after corrective measures have been set out. The Data Protection Officer will require evidence of actions being implemented or rejected which will be stored as part of the investigation file.

5.6 The Data Protection Officer will determine within 72 hours of an incident occurring whether it needs to be reported to the Information Commissioners Office. Consideration of notification to the Information Commissioner is done in line with the ICO guidance of reporting breaches of personal data.

5.7 The Data Protection Officer will consider the rights and freedoms of data subjects when investigating breaches and make a decision as to whether the individuals should be informed of the compromise of their information.

5.8 The Data Protection Officer will manage all complaints received from the Information Commissioners Office and where appropriate will issue any questions or requests to the appropriate Council officers, who will be required to provide the necessary information as instructed.

6 Follow up & Escalation of Actions

6.1 Any actions that arise from incidents will be passed onto the Head Teacher and Governing Body for consideration. These actions must be implemented to mitigate the risk of future incidents, however the school as the data controller is ultimately responsible for determining how actions will be taken forward.

6.2 The Information Governance Schools Officer will follow up completion of these actions within the timeframes set out in the investigation reports.

Monitoring the Effectiveness of the Policy

Annually the effectiveness of this policy will be reviewed annually, or when the need arises, and the necessary recommendations for improvement will be made to the governors.

Mrs. E. Prescott
Headteacher

Mr. D. Corp
Chair of Governors

Date: March 2026