Cotsford Primary School

Data Breach Policy & Procedure

April 2026

Issue date	**April 2026**
Approved by governing body	Yes
Review Cycle	Every 2 years or as legislation or need arises
Next review date	April 2028
Staff responsible	Data Protection Officer
Circulation Details	All staff, Governors

Policy Statement

1. Schools process large volumes of personal and special category data. The school takes all reasonable steps to ensure personal data is handled securely and to prevent personal data breaches.

In the event of a suspected or actual personal data breach, the school will take immediate and appropriate action to minimise any risk to individuals and to comply with its legal obligations under UK GDPR and the Data Protection Act 2018.

Purpose

2. This procedure sets out the process to be followed by staff and governors when a suspected or actual personal data breach occurs.

It provides a clear framework for:

- Reporting and logging breaches
- Containing and investigating incidents
- Assessing risk to individuals
- Determining whether notification to the Information Commissioner's Office (ICO) and/or affected individuals is required

Scope

3. This procedure applies to all personal data processed by the school, including:

- Pupil data
- Staff data
- Parent/carer data
- Governor data
- Visitor data

This includes both electronic and paper records.

Definitions

Term	Definition
Personal data	Any information relating to an identified or identifiable living individual, including name (including initials), identification number, location data or online identifiers such as username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special category data	More sensitive data requiring additional protection, including information about: • Racial or ethnic origin • Political opinions

	• Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Any operation performed on personal data, including collection, organising, structuring, storage, adapting, altering, retrieving, using, sharing, erasing or deletion. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held processed
Data controller	A person or organisation determining the purposes and means of processing personal data (the school)
Data processor	A third-party processing data on behalf of the school
Data subject	The individual whose data is processed
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
ICO	Information Commissioner's Office (UK regulator for data protection)
Phishing / social engineering	Attempts to obtain confidential information through deception
Ransomware	Malicious software used to block access to data until payment is made

Legal Context

4. The UK GDPR and Data Protection Act 2018 regulate the processing of personal data.
5. Under Article 5(1)(f) of the UK GDPR, personal data must be:

"processed in a manner that ensures appropriate security… including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage."

6. Under Articles 33 and 34 of the UK GDPR:

    - Personal data breaches must be reported to the ICO within **72 hours** where there is a risk to individuals
    - Individuals must be informed where there is a **high risk to their rights and freedoms**

What is a personal data breach?

7. A personal data breach occurs when personal data is:

- Lost
- Stolen
- Accessed without authorisation
- Shared incorrectly
- Altered or destroyed unlawfully

This includes both accidental and deliberate incidents.

Examples of personal data breaches

8. Examples include (but are not limited to):

    - Email sent to the wrong recipient
    - Loss or theft of devices (laptops, USBs)
    - Unauthorised access to records
    - Publishing personal data accidentally
    - Verbal disclosure in public areas
    - Failure to redact documents
    - Cyber attacks (e.g. ransomware, phishing)

ICT-related breaches

9. Where a breach involves ICT systems or devices, technical advice must be sought immediately from the school's IT provider.

Mandatory Procedure

10. All breaches must follow four key stages:

    - **Reporting**
    - **Containment and recovery**
    - **Investigation and risk assessment**
    - **Evaluation and response**

Stage 1: Reporting

Responsible: Staff → Headteacher → DPO

11. Any staff member who identifies a potential breach must:

    - Act immediately to contain the breach
    - Report it **without delay (same day)** to the Headteacher and DPO

12. The following must be recorded:

    - Date/time of incident
    - Nature of breach
    - Type of data involved
    - Number of individuals affected

- Security measures in place
- Actions taken

13. All incidents must be logged, including near misses.

Stage 2: Containment and recovery

Responsible: Headteacher / DPO

14. Immediate steps must be taken to:

    - Recover data where possible
    - Prevent further access
    - Secure systems

15. If the breach is fully contained (e.g. email recalled unopened), it may be recorded as a **near miss**.
16. Safeguarding takes priority — if a pupil is at risk, safeguarding procedures must be followed immediately.

Stage 3: Investigation and risk assessment

Responsible: DPO / Headteacher / Chair of Governors

17. A formal investigation is required where:

    - Data has been accessed or disclosed
    - Data is lost or cannot be recovered
    - Sensitive data is involved
    - There is risk of harm to individuals

18. The investigation must consider:

    - Cause of the breach
    - Type and sensitivity of data
    - Number and vulnerability of individuals affected
    - Likely consequences (e.g. harm, distress, identity theft)

Key Decisions

19. The school must determine:

    - Whether affected individuals should be informed
    - Whether the ICO must be notified
    - Whether the breach is a **formal reportable breach**

Stage 4: Notification

ICO Notification

20. The ICO must be notified within **72 hours** if the breach is likely to result in a risk to individuals.

Notification to individuals

21. Individuals must be informed where there is a **high risk**, including:

    - Risk of identity theft
    - Financial loss
    - Safeguarding concerns
    - Reputational damage

Assessing severity of breach

22. When determining severity, the school will consider:

    - Type of data (e.g. medical, safeguarding)
    - Sensitivity
    - Number of individuals affected
    - Vulnerability of individuals (e.g. children)
    - Whether data is in the public domain

23. The risk to individuals is the key deciding factor.

Near miss vs breach vs reportable breach

Near Miss

- Breach contained
- No data accessed
- No risk to individuals

Data Breach

- Data compromised
- Limited impact
- May not require ICO notification

Reportable Breach

- High risk to individuals
- Requires ICO notification
- May require informing individuals

UK GDPR data breach reporting (DPA 2018) | ICO

Final evaluation and response

24. Following investigation, the school will:

- Identify root causes
- Implement corrective actions
- Update procedures
- Provide staff training

25. Findings will be reported to the governing body.

Disciplinary considerations

26. Where appropriate, breaches may result in disciplinary action in line with school policies.

Serious breaches may involve:

- Referral to LADO (where safeguarding concerns arise)
- External investigation

Record keeping

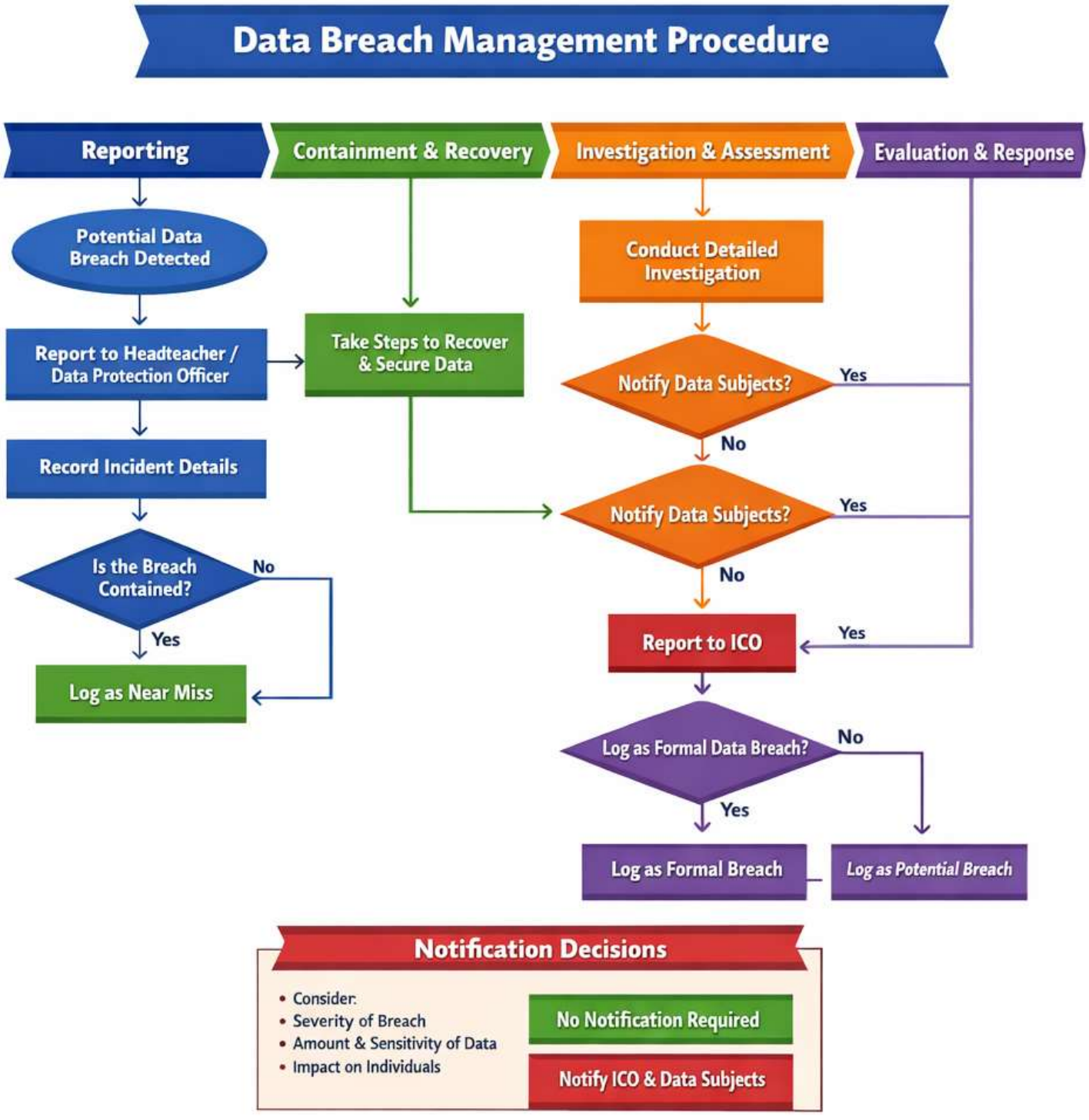
27. The school will maintain a **data breach log**, including:

- All incidents (including near misses)
- Investigation outcomes
- Actions taken

This supports accountability under UK GDPR.

The procedure is summarised on Appendix 1 for quick reference.

Appendix 1


Data Breach Management Procedure
Reporting
Containment & Recovery
Investigation & Assessment
Evaluation & Response
Potential Data Breach Detected
Report to Headteacher / Data Protection Officer
Record Incident Details
Is the Breach Contained?
No
Yes
Log as Near Miss
Take Steps to Recover & Secure Data
Conduct Detailed Investigation
Notify Data Subjects?
Yes
No
Notify Data Subjects?
Yes
No
Report to ICO
Yes
Log as Formal Data Breach?
No
Yes
Log as Formal Breach
Log as Potential Breach
Notification Decisions
• Consider:
• Severity of Breach
• Amount & Sensitivity of Data
• Impact on Individuals
No Notification Required
Notify ICO & Data Subjects