DATA PROTECTION BREACH PROCEDURE

1. Introduction

1.1 The Data Breach Form at Appendix A must be completed and updated as the process progresses.

1.2 The Data Breach Flowchart at Appendix B outlines the process to be followed.

1.3 A Data Breach Log is held by the Trust and all breaches should be reported to the Governance and Compliance Officer.

1.4 Most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

2. Data Breaches

2.1 If a breach occurs it will be swiftly reported. Examples of breaches include:

- Information being posted to an incorrect address which results in an unintended recipient reading that information.
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar.
- Sending an email with personal data to the wrong person.
- Dropping or leaving documents containing personal data in a public place.
- Personal data being left unattended at a printer enabling unauthorised persons to read that information.
- Not securing documents containing personal data (at home or work) when left unattended.
- Anything that enables an unauthorised individual access to school buildings or computer systems.
- Discussing personal data with someone not entitled to it, either by phone or in person.
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to equipment and records being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

3. Action to be taken

3.1 Explain what has been lost or potentially accessed. This an important element of working with the Information Commissioner's Office (ICO) and necessary to mitigate the impact.

3.2 Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

3.3 The breach must be immediately reported to the Headteacher, the Data Protection Officer and the Trust Governance and Compliance Officer.

3.4 The breach notification form will be completed and the breach register updated.

3.5 The breach report will be reported to the ICI within 72 hours of becoming aware of the breach. It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

3.6 If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people this will be done in a co-ordinated manner with support from the Data Protection Officer.

4. Procedure

4.1 For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

4.2 The breach and process will be described in clear and plain language.

4.3 If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Headteacher/CEO with support from the Trust Governance and Compliance Officer and the Data Protection Officer.

4.4 Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

4.5 A post breach action plan will be put into place and reviewed.

5. Evidence Collection

5.1 It may be necessary to collect information about how an information security breach or unauthorised release of data occurred.

5.2 This evidence gathering process may be used as an internal process it may be a source of information for the ICO, it could also be used within disciplinary, criminal or civil proceedings.

5.3 This process will be normally conducted by a suitable member of school staff. This may be the Trust Governance and Compliance Officer or Data Protection Officer, depending on the nature of the breach.

5.4 Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

5.5 A record of what evidence has been gathered, stored and secured will be available as a separate log.

Document management

Review cycle:	Every two years
Next review due:	May 2022
Policy owner	Head of HR

Appendix A DATA BREACH NOTIFICATION FORM

1. **When did the breach occur (or become known)?**

2. **Who was involved?**

3. **Who was this reported to?**

4. **Date and time it was reported**

5. **Date and time DPO notified**

6. **A description of the nature of the breach. This must include the type of information that was lost, e.g. name, address, medical information, NI numbers.**

7. **The categories of personal data affected e.g. electronic, hard copy**

8. **Approximate number of data subjects affected.**

9. **Approximate number of personal data records affected**

10. **Name and contact details of the Data Protection Officer / GDPR Owner.**

11. **Consequences of the breach. What are the potential risks?**

12. **Any measures taken to address the breach. What actions and timeline have been identified?**

13. **Any information relating to the data breach**

Two Counties Trust

Appendix B BREACH MANAGEMENT FLOWCHART