Shefford Lower School

Data Breach Policy

Written by	Reviewed & Ratified by Governors	Shared with Staff	Last Updated	Review cyle	Next Review Due
Victoria Joyce Business Manager	November 2024	November 2024	November 2024	Annual	November 2025

1. Aims and objectives

1.1 This policy sets out:

- Policy statement on data breaches
- Definitions
- Reporting responsibilities

1.2 This policy aims to ensure that adequate controls are in place so that:

- Data breaches are identified, and action is taken quickly. Actions should be proportionate, consistent and transparent
- An assessment is completed to ensure that any major data breaches are reported to the Senior Management Team (SMT), Data Protection Officer (DPO) and the ICO appropriately
- All data breaches and near misses are recorded and regularly reported
- Lessons are learnt to seek to ensure similar mistakes are not repeated by putting in place appropriate control mechanisms and passing on learning.

1.3 This policy is in place to ensure that all staff can identify a data breach and understand the steps required for assessing and dealing with them.

1.4 This policy identifies inherent risk of a data breach and/or near-miss, which will ensure that senior management and our DPO are informed as appropriate, able to manage actions relating to any real or potential serious data breach and be able to report to the ICO and affected individuals as appropriate.

2. Legislation

2.1 The General Data Protection Act 2018, the Data Protection Act 2018 (DPA) as amended by UK GDPR 2021 is based around six principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on organisations that are responsible for processing it.

2.2 Occasionally things will go wrong, and mistakes will be made. Sometimes this may entail significant financial or reputational risk for schools and students. It is vital that we can identify, evaluate contain data breaches as soon as they occur.

2.3 Identifying data breaches quickly and effectively to limit any impact on our students is critical. Equally we need to understand where there are areas of weakness within our operating processes and continuously improve to reduce the risk of failures leading to data breaches.

3. Definitions

3.1 What is a data breach?

3.1.1 According to the ICO organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

3.1.2 A data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

3.1.3 A personal data breach may mean that someone outside the school gets unauthorised access to personal and/or special category (sensitive) data. But a personal data breach can also occur if there is unauthorised access within the school for example an employee accidentally or deliberately accesses information, they have no need to know, alters or deletes personal data.

3.1.4 A data security breach can happen for many reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

3.1.5 Human error is the most common cause of data breaches. These can happen for many reasons:

- Theft or loss of paperwork
- Data posted to incorrect recipient
- Data sent by email to incorrect recipient
- Failure to redact personal/sensitive data before it is disclosed.

3.2 What is a near miss?

3.1.1 A near miss is an event that does not result in a data breach, but which had the potential to do so. Examples of such events might include data that was misplaced but found quickly internally or data that was sent out but was identified and returned without it having been accessed by anyone.

3.1.2 Our school is committed to identifying weaknesses in our procedures. We will record all near misses to understand patterns, implement improvements and report to senior management and governors.

4 Training

4.1 Mandatory training will be provided to all staff on data protection compliance.

4.2 Training will be provided to all new employees including temporary and contracted staff.

4.3 All employees will undertake refresher training annually.

5 Identification

5.1 Data breaches or near misses may be identified as part of everyday business. They may be identified by the recipient as the first point of contact; by a parent or pupil making us aware; by a third party like the local authority making us aware.

5.2 Where a data breach is identified the schools' designated member of staff, and the Data Protection Officer must be informed immediately. The school data protection lead (with support from the Data Protection Officer) will investigate the occurrence, complete the Data Breach Form and deicide upon actions and lessons to be learnt.

6 Risk Assessments

6.1 When a data breach is identified and reported to your DPO a risk assessment will be completed by the DPO.

6.2 The DPO will be available to support the data protection lead in the school. Advice and guidance will be provided on managing the containment and recovery of any lost data and will support the investigation process. However, the data protection lead within the school will maintain overall ownership throughout.

NOTE: data breaches should be reported immediately so the school can take action to minimise any potential risks arising from the breach. All incidents should also be reported to the Data Protection Officer who will advise how best to deal with the case and assess the risk of harm to determine whether it needs to be reported to the ICO. It is a mandatory requirement that serious incidents are reported within a 72-hour timescale.

7 Containment and recovery

7.1 Containment and recovery involve limiting the scope and impact of the data breach and stemming it as quickly as possible. Where data can be recovered, all reasonable steps should be taken to do so.

7.2 The data breach owner, with support from the DPO, must quickly take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage. Steps might include:

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Contacting the Admin Office and other key departments so that they are prepared for any potentially inappropriate enquiries about the affected data subjects
- The data protection lead, with the approval of the Senior Management Team, for a school-wide email to be sent
- Contacting the Admin Office so they can be prepared to handle any press enquiries or to make any press releases
- The use of back-ups to restore lost, damaged or stolen information
- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

8 Investigation

8.1 If a data breach is identified, then a formal investigation should be commenced by the designated member of staff (data protection lead) who should determine the seriousness of the breach and the risks arising from it. Specifically, the data breach owner should identify:

- Whose information was involved in the breach and the nature of that information, how sensitive is it?
- What went wrong
- The potential affect on the data subject(s)
- What immediate steps are required to remedy the situation and will this and or reduce this risk
- What lessons have been learnt to avoid a repeat incident.

To support this process, the data breach owner should complete the Data Breach Report form.

8.2 The investigation should consider:

- The type of information
- Its sensitivity
- How many individuals are affected by the breach?
- What protections are in place (e.g. encryption)?
- What happened to the information?
- Whether the information could be put to any illegal or inappropriate use
- What could the information tell a third party about the individual?
- What types of people have been affected (the students, parents, staff etc)?
- Whether those affected have any special needs/vulnerabilities.

NOTE: Actions to contain and recover data as well as mitigate any risk should be taken immediately. The initial investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered / reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

8.3 Advice, input and support should be sought from your Data Protection Officer throughout this process.

9 Informing affected individuals

9.1 The ICO requires us to inform those affected where there is a significant breach of personal and sensitive data and the risk of harm to those individuals is high.

9.2 Clearly if there was a high risk of further harm the school would have an obligation to disclose the breach to each individual affected. However, this must be balanced against the risk of causing further distress and anxiety to the families by informing them about the breach.

9.3 Only the data protection lead and DPO can decide whether to advise affected individuals of a data breach and therefore the reasons for deciding to do this should be clearly set out in the investigation report and discussed with the data breach owner and other involved parties before affected parties are informed.

10 Learning lessons

10.1 The Lessons Learnt Action Plan for data breaches and near misses should be completed and will form part of the investigation process.

10.2 The action plan should clearly outline the lessons learnt, the controls agreed to reduce the risk of a further reoccurrence, a lead member of staff to complete each action and a completion date.

10.3 The case will not be considered closed until all actions agreed have been completed.

11 Data breach Log

11.1 All data breaches, including near misses, will be recorded on the Data Breach Log.

11.2 This information will be reviewed and analysed at least annually to identify patterns and monitor the implementation of agreed service improvements.

11.3 The DPO will collate all data breach reports and will report trends and lessons learnt to SMT.