Personal Data Breach Policy and Procedures

Version:	2
Date Issued:	17/10/2024
Date of Previous Issue:	08/2022
Approved by:	Governing Body
Date Approved:	17/10/2024
Review Date:	17/10/2026

Signatures:

	Name	Signature
Chair of Governors:	**Jess Williams**	J. Williams
Headteacher:	**Sarah Court**	S. Court

Table of Contents

1. Introduction and Policy Statement:

1.1. The School processes personal data about staff, pupils, parents and other individuals who come into contact with the School in order to provide education and other associated functions.

1.2. A personal data breach occurs when, as defined in Article 4 of the UK General Data Protection Regulations (GDPR), a breach of security leads to the accidental or unlawful; destruction, loss, alteration, unauthorised disclosure of, or access to that personal data transmitted, stored or otherwise processed.

1.3. The Personal Data Breach Policy and Procedures document is connected to the School's overarching Data Protection Policy.

2. Policy Purpose:

2.1. This policy is intended to ensure that a personal data breach is managed in the most appropriate way in line with data protection legislation and that all staff are aware of their obligation to manage a personal data breach properly.

2.2. Examples of a personal data breach that may occur within our Schools setting include:

2.2.1. An unauthorised individual accessing our systems or records containing personal information;

2.2.2. Disclosing personal information to the wrong person in an email, letter, instant message etc;

2.2.3. Alteration or deletion of personal information by a member of staff without a business need or authorisation to do;

2.2.4. Personal information not being available when required, and this unavailability has a significant negative affect on individuals;

2.2.5. Cyber security incidents effecting the personal information contained within our computer systems

2.3. This policy sets out the procedures that the School will follow when managing a personal data breach.

3. Scope of Policy:

3.1. This policy applies to all School staff who must understand the procedures to manage a personal data breach.

3.2. Contracted third parties should be aware of their requirements to report any personal data breach back to the School when that breach has compromised School data – these requirements will be set out within the contract between the School and third party.

4. UK GDPR Personal Data Breach Requirements:

4.1. In the case of a personal data breach and in line with Article 33 (in accordance with data protection principles under Article 5) of the UK GDPR, the School shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office (ICO), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual.

4.2. In the case of a personal data breach and in line with Article 34 (in accordance with data protection principles under Article 5) of the UK GDPR, the School will communicate a personal data breach to a data subject when it is likely to result in a high risk to the rights and freedoms of that data subject.

4.3. The School will liaise directly with the Data Protection Officer (DPO) to establish whether a personal data breach should or should not be reported to the ICO and the data subject.

5. Personal Data Breach Procedures:

5.1. Step 1: Identify the personal data breach and inform the DPO:

5.1.1. A personal data breach is identified when it is confirmed that the incident meets the definition of a personal data breach as outlined in point 1.2. above.

5.1.2. The School shall inform the DPO of the breach regardless of the level of seriousness and will begin to determine the answer to all questions posed in Appendix 2 below.

5.1.3. The School will provide the DPO with all known and relevant details surrounding the personal data breach and indicate the level of risk to an individual. This includes information on:

5.1.3.1. The number of data subjects involved;
5.1.3.2. What personal data is involved;
5.1.3.3. When the personal data breach happened;
5.1.3.4. How the personal data breach was caused;
5.1.3.5. Context surrounding the personal data breach;
5.1.3.6. Other details that are deemed useful (This will vary from incident to incident).

5.1.4. The DPO can help the School assess this risk based on the information supplied and advise accordingly.

5.2. Step 2: Contain the personal data breach:

5.2.1. Once a personal data breach has been identified as having occurred the School will where possible attempt to contain any personal data breaches within reasonable efforts.

5.2.2. Reasonable efforts might include, for example, attempting to recall sent emails; immediately contacting incorrect recipients and asking them to delete or destroy information that has been accidentally provided to them; collecting erroneously issued documentation, or any other efforts that could be defined as reasonable to be carried out at the time.

5.2.3. The School will not attempt to contain a personal data breach where certain professional expertise is required, for example, ICT staff.

5.2.4. If it is not possible to contain the personal data breach immediately, then reasonable efforts will continue until the information has been contained appropriately, whether it be returned, deleted or destroyed.

5.2.5. When considering the impact of the incident, then consideration must be given to all possible consequences, no matter how trivial or extreme.

5.3. Step 3: Investigate the personal data breach and assess the risks to all individuals involved:

5.3.1. The School will investigate each personal data breach to try and identify the "*WHAT, WHY, WHEN & WHO*":

5.3.1.1. WHAT: What has happened, what information has been breached, what have we put in place to mitigate a reoccurrence?
5.3.1.2. WHY: Why and how did it happen?
5.3.1.3. WHEN: When did the incident occur?
5.3.1.4. WHO: Who caused it, who is likely to be affected, who has been affected?

5.3.2. The School will assess the risks associated with each personal data breach and, where high risks have been identified, determine whether the incident is reportable to the ICO in liaison with the DPO.

5.3.3. The DPO can help the School identify and score all risks via the Incident risk assessment, which documents grading the risk impact and likelihood between 1 and 5, 1 being the lowest and 5 being the highest impact (See Appendix 1 below).

5.3.4. Risks Scored between 6 – 25 (yellow & red) requires reporting to the ICO.

5.3.5. The data subjects must be informed by the School when the impact has been scored as 3 from the Figure 2 impact descriptions below.

5.4. Step 4: Report (if necessary) a personal data breach to the ICO and inform (if necessary) data subjects:

5.4.1. The DPO will have final decision over the reporting of all personal data breaches, which occurred within the School, to the ICO within 72 hours after the School became aware of the incident

5.4.2. An investigation report will need to be developed by the School to document the actions of the School in response to the breach, and if necessary, further inform the ICO to assist with their decision making. The report should include:

5.4.2.1. A timeline of events including the breach and actions taken after;
5.4.2.2. Details of all parties involved and affected;
5.4.2.3. Details of the personal data disclosed or compromised;
5.4.2.4. Mitigation (what did the School do to try and prevent it), such as processes in place, training received etc.;
5.4.2.5. Whether any policies or procedures are in place that should have been followed.
5.4.2.6. Recommendations (what the School will do to prevent it from happening again).

5.4.3. Where personal data breach risk assessments have not reached the threshold of reporting to the ICO, the School will continue to manage the personal data breach and mitigate the risk of reoccurrence.

5.5. Step 5: Mitigate and reduce the risk of a similar personal data breach occurring:

5.5.1. The School will look to mitigate similar personal data breaches from occurring by considering which procedures or processes failed for the specific personal data breach, and what could be implemented to improve the procedure or process to reduce the risk of recurrence.

5.5.2. For example, if a member of staff sent out an email to an incorrect recipient, and through an investigation it was identified that they had relied upon an “auto-fill” feature within their email system, then the School may

consider turning off that specific feature across the School's digital environment for all users or provide awareness as to the consequences of errors.

5.5.3. The outcomes of any personal data breach investigation will be recorded by the School.

5.5.4. The School and DPO will only consider a personal data breach record as 'closed' when the information has been contained, or the threat of risk has reduced to a tolerable level, and includes implementing mitigating actions.

5.6. Step 6: Lessons learnt and recommendations:

5.6.1. The School will consider all recommendations from the investigation report, the DPO and the ICO and will consider the implementation of recommendations if not done so already, documenting where recommendations are rejected, seeking advice from the DPO in the process.

5.6.2. The School will also reflect on the detailed report written for the ICO to determine whether there are other lessons to be learnt.

(Scroll down for Appendix 1)

6. Appendix 1: Risk Assessment Descriptions.

Figure 1 - Likelihood descriptions

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Figure 2 - Impact Descriptions

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Figure 3 - Breach Assessment Grid

Severity of Impact	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that rights have been affected.				

(Scroll down for Appendix 2)

7. Appendix 2: Checklist:

7.1. For each step of the personal data breach procedure, it's good practice to ask questions such as:

- Identification:
  - Does the incident include personal information?
  - Has the incident affected the *integrity*, *availability* or *confidentiality* of personal information?
  - Does the personal information affected belong to the School?
  - Has an incident increased the likelihood that an individual will experience a significant consequence?
  - Have the School alerted the DPO (if you have identified a personal data breach)?

- Contain:
  - Can I recall an email that has gone to the wrong email address?
  - Can I correct incorrect information held on a system?
  - Can I stop a letter with an incorrect address from leaving School premises?
  - Can I call an individual who is in receipt of someone else's personal information to ask that an email is deleted, or a letter destroyed?

- Investigate:
  - Have I asked the right questions?
    - Have I determined the "WHAT"?
    - Have I determined the "Why"?
    - Have I determined the "When"?
    - Have I determined the "Who"?
  - Have I identified all risks?
  - Have I assessed all risks?
  - Have I provided all details to the DPO?

- Report:
  - Have I determined and indicated the risks to the DPO?
  - Is the ICO being notified of the personal data breach?
  - Will the data subject need to be informed?

- Mitigate:
  - Have I identified that a breach has occurred due to a failure of processes or procedures?
  - Can the School put something in place or strengthen a current process to prevent reoccurrence?
  - Have I documented how the School will improve a process that has failed?

- Learn:
    - Are there any clear and obvious lessons to be learnt?
    - Have you documented those lessons and thought of ways to implement them?
    - Where appropriate, have all staff been made aware of mitigation actions?