Personal Data Breach Procedure Policy

(to be read with Data Protection Policy and PCC Data Breach Guidance)

Policy adopted by the Governing Body 2022

Signed H.A Nixon

Head Teacher

Phil Hobbs

Chair Of Governors

Table of Contents:

1. Introduction to the Policy:

1.1. The school collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

1.2. Sometimes, the security of personal data can be compromised which can lead to personal data breaches, which is the unlawful, mostly accidental, and inappropriate disclosure of personal information.

1.3. As defined in the UK GDPR (Article 4(12)), a personal 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." Examples of this are:

1.3.1. Access to information by those not authorised;
1.3.2. Deliberate action by a member of staff or a contractor;
1.3.3. Sending information contained in emails, letters, messages etc. to the wrong address;
1.3.4. Laptops, USB, CDs etc. being lost or stolen;
1.3.5. Alteration or deletion of personal data without authorisation;
1.3.6. Information not being available when required, and this unavailability has a significant negative affect on individuals.
1.3.7. Cyber incidents effecting the personal data contained within computer systems

1.4. The personal data breach procedure policy details the School's actions should they identify that the security of personal information, of which they are the controller has been compromised.

2. Procedure Overview:

2.1. The following procedure tries to manage all aspects of a personal data breach, including the identification of a breach, the investigation of that breach, and the notification of relevant professionals (The Data Protection Officer) and documentation (administration):

2.2. Step 1: Identify the Personal Data Breach;

Step 2: Contain the Personal Data Breach;

Step 3: Investigate the Personal Data Breach;

Step 4: (If appropriate) Report and Inform;

Step 5: Mitigate and reduce the risk of reoccurrence.

2.3. It must be noted that the procedure might be followed differently in certain circumstances, for example when the risk of reoccurrence is high, the School may decide to mitigate that risk immediately, therefore Step 5 becomes the second step.

3. (Step 1): Identify the Personal Data Breach & Inform the Data Protection Officer (DPO):

3.1. A personal data breach is identified when it is confirmed that the incident meets the definition of a personal data breach outlined in point 1.3. above.

3.2. The School shall inform the School's Data Protection Officer (DPO) of the breach regardless of the level of seriousness.

3.3. The School will provide the DPO with all known and relevant details surrounding the personal data breach that can be used to help the DPO assess the risks the breach possess to data subjects involved and the seriousness of the breach itself. This includes information on:

3.3.1. The number of data subjects involved;
3.3.2. What personal data is involved;
3.3.3. When the personal data breach happened;
3.3.4. How the personal data breach was caused;
3.3.5. Context surrounding the personal data breach;
3.3.6. Other details that are deemed useful (This will vary from incident to incident).

3.4. All identified personal data breaches and security incident details will be recorded centrally by the School within, for example, a Microsoft Excel Spreadsheet. For all incidents, recorded details at a minimum will include: the nature of the incident, time and date of the incident, whether or not the breached information has been contained, whether or not it has been reported (to the ICO or data subjects involved/affected) and mitigation steps.

4. (Step 2): Contain the Personal Data Breach:

4.1. Once a personal data breach has been identified, the School will where possible attempt to contain any personal data breaches that has been identified immediately, within reasonable efforts.

4.1.1. 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; or any other efforts that could be defined as reasonable to be carried out at the time.
4.1.2. Unreasonable efforts might include, for example, attempting to fix computer systems or other ICT-based applications that have been hacked or compromised. The School will not attempt to contain a personal data breach where certain professional expertise is required, for example, ICT staff.

4.2. 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.

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

5. (Step 3): Investigate the Personal Data Breach and Assess the Risks to all Individuals Involved:

5.1. The School will investigate each personal data breach to try and identify the “WHAT, WHY, WHEN & WHO”:

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

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

5.3. The DPO can help the School identify and score all risks via the DPO’s risk assessment, which looks at grading the risk impact and likelihood between 1 and 5, 1 being the lowest and 5 being the highest impact (See **Appendix 1** below):

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

5.3.2. The individual **must** be informed when the impact has been scored as 3 from the *Figure 2 impact descriptions* below.

6. Step 4): Reporting a Personal Data Breach to the Information Commissioners Office (ICO) and informing the Data Subject(s):

6.1. The DPO will report all personal data breaches, which occurred within the School, that have been scored 6 or higher on the DPO's risk assessment (Appendix 1) to the ICO within 72 hours after the School becoming aware of the incident via the ICO's reporting template online www.ICO.co.uk.

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

6.1.2. A detailed report will need to be written by the School to further inform the ICO of the entire personal data breach events, which should include:

- A timeline;
- Details of **all** involved;
- Details of the data disclosed or compromised;
- Mitigation (what did the School do to try and prevent it);
- Whether any policies or procedures are in place that should have been followed;
- Recommendations (what the School will do to prevent it from happening again).

6.2. The DPO will not report personal data breaches to the ICO, which occurred within the School, that have been scored 5 or lower on the DPO's risk assessment. The School will continue to manage the personal data breach and mitigate the risk of reoccurrence.

6.3. Best practice advises that all personal data breaches should be notified to the individual. However, the individual **must** be informed when the impact has been scored as 3 from the *Figure 2 impact descriptions* below.

7. (Step 5): Mitigate and reduce the Risk of a similar Personal Data Breach occurring:

7.1. Before accepting that a personal data breach record is 'closed' 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 and reduce the risk of recurrence.

7.1.1. For example, if a breach was caused by the School's administration process whereby a letter was sent to the incorrect recipient due to the fact a 'postal checking regime' was not followed, then the School might implement a postal checking log system that enforces appropriate secondary checks to addresses on a letter.

7.2. All outcomes of any personal data breach will be recorded by the School.

7.3. The School will only consider a personal data breach record as 'closed' when the information has been contained, or the threat of risk has reduced to nil, including implementing mitigation actions.

8. (Step 6): Reflect, and Lessons Learnt:

8.1. The School will consider all recommendations and notices issued by the ICO and will implement suggested actions if not done so already – seeking advice from the DPO in the process.

8.2. The School will consider all recommendations provided by the DPO and will implement suggested actions if not done so already.

8.3. The School will also identify where changes can be made to prevent reoccurrence.

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

Appendices

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.				

Appendix 2: Checklist:

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?

ENDS