DATA BREACH POLICY

Approved by:	**Resource Committee**	**Date: 24/06/2026**
Last reviewed on:	**June 2026 (Full Governing Body ratified July 2026)**	
Next review by:	**Upon DPO advice**	

Rationale:
Silverwood School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This policy applies to all personal and sensitive data held by Silverwood School and all school staff, governors, volunteers and contractors, referred to herein after as 'staff'.

Aims and Objectives:
The aims of our Data Protection Policy encompass the following:

Morality	To foster an ethos of trust within the school where all who handle personal data do so within the framework of the law. To ensure that confidentiality is a whole school issue and that in lessons ground rules are set for the protection of all. To ensure that if there are child protection issues then the Correct procedure is followed as outlined in the school's Child Protection Policy.
Communication	To ensure that staff, parents, and pupils are aware of the School's Data Protection Policy and procedures and how personal data should be processed, stored, archived and deleted/destroyed. To provide consistent messages in school about handling information about children, staff, and families once it has been received. To ensure that children/parents know that school staff cannot offer unconditional confidentiality
Co-operation	To reassure those associated with the school that their best interest will be maintained. To ensure that staff and parents have a right to access to all records held on them or their child(ren), except where the sharing of these could endanger the child.
Respect	To protect personal data at all times and to give all school staff clear, unambiguous guidance as to their legal and professional roles and to ensure good practice throughout the school which is understood by children, parents/carers and staff. To ensure that there is equality of provision and access for all including rigorous monitoring of cultural, gender and special educational needs.

3. Purpose

This data breach policy sets out the course of action to be followed by all staff at Silverwood School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller 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 supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
   (a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
   (b) Communicate the name and contact details of the data protection officer (who can be contacted through the school) or other contact point where more information can be obtained
   (c) Describe the likely consequences of the personal data breach
   (d) Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

For more detailed procedure see the Silverwood School Personal Data Breach Procedure.

4. Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Poor data destruction procedures
- Human error
- Cyber-attack
- Hacking

Managing a Data Breach

In the event that the school identified or is notified of a personal data breach, fhe following steps should be followed –

1. The person who discovers/receives a report of a breach must inform the Headteacher or, in their absence, the Director of Finance & Resources and the school's Data Protection Officer (DPO). If the

breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Headteacher/DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.
3. The Headteacher/DPO must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.
4. The Headteacher/DPO must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.
5. The Headteacher/DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment
b. Contacting the relevant Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Headteacher/DPO.
c. The use of back-ups to restore lost/damaged/stolen data
d. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
e. If the data breach includes an entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

5. Investigation

In most cases, the next stage would be for the Headteacher/DPO to fully investigate the breach. The Headteacher/DPO should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider –

- The type of data
- Its sensitivity
- What protections were in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable

personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter had been resolved.

6. Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Headteacher/DPO should, after seeking expert of legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individual, give specific and clear advice on what they can do to protect themselves and what the school is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

7. Review and Evaluation

Once the initial aftermath of the breach is over, the Headteacher/DPO should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Leadership Team meeting and Full Governors Meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put this right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with HR or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

8. Implementation

The Headteacher/DPO should ensure that staff are aware of the School's Data Protection Policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the school's Data Protection Policy and associated procedures, they should discuss this with their line manager, DPO or the Headteacher.

Staff should be alert to the potential of accidental data breaches in their day to day practice. In addition to written, photographic and electronic data they should also be mindful of the confidentiality within their conversations and where these occur.

It is the responsibility of the school's Data Protection Controllers (DPC) to maintain logs of near misses and accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy for example. The purpose of this log, particularly for near misses is to

- Enable the school and employees to learn from incidents

Within ongoing logs it is essential that the following aspects are identified:

- The "responsible person" for each incident
- The communications plan, including escalation procedures where applicable
- The results of any action for rapid resolution

- A plan of action of non-recurrence and further awareness raising

The DPC and the DPO should meet at least termly to review these logs with a view to using incidents as opportunities to learn from practice that had the potential to cause a breach.
All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based on this policy and communication plan.