Data Protection Policy

Last Reviewed Date:	23/09/2024	Reviewed:	30/07/2025

School Business Manager:		**Date:**	30/07/2025
Headteacher:		**Date:**	11/09/2025

Date of Next Review:	September 2026

C O N T E N T S

1. General Statement

Amwell View School takes the privacy of our staff, governors, parents/guardians and pupils very seriously and work to the highest standard to keep your data safe in-line with the General Data Protection Regulation (GDPR).

We are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information we collect and process in accordance with the GDPR and the Data Protection Act 2018.

As a school, we are a Data Controller under the regulations and as such define how and why personal data is collected, stored, and used. We also utilise Data Processors – third parties that process the data we control on our behalf. As a Data Controller, we must comply with the regulation as well as ensuring that all of our Data Processors are compliant.

We will achieve compliance by ensuring personal data is processed lawfully, transparently, and for a specific purpose. Once the purpose is fulfilled and the data is no longer required, it will be deleted, as stipulated within our Records Management Policy and Retention Schedule.

2. Enquiries

Information about the school's Data Protection Policy is available by contacting the Data Protection Officer (DPO) by letter at the school's address or electronically by email: **dpo@amwell.herts.sch.uk**.

General information about the Data Protection Act can be obtained from the Data Protection Commissioner (website https://www.gov.uk/data-protection).

General information about GDPR can be obtained from the Information Commissioner's Office (website https://ico.org.uk).

3. Fair Obtaining and Processing

Amwell View School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

- **processing** - means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
- **data subject** -the person that the data relates to.
- **personal data** - means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
- **parent** has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.
- **data item** – a single piece of information about a data subject.
- **data item group / element** – a group of data items that are typically captured about the same activity or business process in school.
- **system** – a piece of software, computer package or manually managed asset that supports the administration of one or more areas of school life.
- **system group** – an umbrella term to describe the areas of school administration where systems that contain personal level data typically reside.

4. Lawful Basis

The school is registered under the Data Protection Act for holding personal data. The lawful basis on which we collect this information is Article 6(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller and Article 9 (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or **statistical** purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights of the interests of the data subject. Information held will not be used for any other purpose without the data subject's consent. Personal data entries are available for inspection, by appointment, at the school office. Explanation of any codes and categories entered is available from the DPO who is the person nominated to deal with data protection issues in the school.

5. Data Integrity

The school undertakes to ensure data integrity by the following methods:

- **Data Accuracy**
  Data held will be as accurate and up-to-date as is reasonably possible. If a data subject informs the School of a change of circumstances their computer record will be updated as soon as is practicable. Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

- **Data Adequacy and Relevance**
  Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. (Details should be added on how and when records are checked for irrelevant data and who has the say on what must be deleted).

- **Length of Time**
  Data held about individuals will not be kept for longer than necessary for the purposes registered. The School Records Management and Retention Schedule is based on the IRMS Information Management Toolkit for Schools Version 6 (2019). It is the duty of the Headteacher to ensure that obsolete data are properly erased.

6. Subject Access

The GDPR ensures there are stronger rights for individuals. All data subjects have a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a Subject Access Request is received the school's policy is that:

- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

7. Processing Subject Access Requests

Subject Access Requests must be made in writing using the Subject Access Request Form (Appendix 1). Completed forms should be submitted to the Data Protection Officer. An entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (eg Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

8. Authorised Disclosures

The school will, in general, only disclose data about individuals with their consent. However there are circumstances under which the school's Headteacher may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities eg in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.
- A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.
- An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

9. Data and Computer Security

Amwell View School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

10. Physical Security

Appropriate building security measures are in place, such as alarms, and deadlocks. Only authorised persons are allowed to use the office server. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied. GPS Tracking with listening-in devices are strictly forbidden to be used within the school premises.

11. Software Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (ie security copies are taken) regularly.

12. Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the Headteacher in consultation with the Governing Body and is monitored and reviewed regularly, especially if a breach becomes apparent. The school's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the school should in the first instance be referred to the Data Protection Officer.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

13. Creation and Management of School Activities

The Amwell View School secure archive is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of school-life among many generations; and to serve as a research resource for all interested in the history of Amwell View School and the community it serves.

14. Appendix 1

SUBJECT ACCESS REQUEST FORM

You may only use this form to make a Subject Access Request to Amwell View School.

The Subject

Title (e.g. Dr, Miss, Mr, Mrs, Ms)	
First Name	
Last Name	
Postal Address	

Your details

Title (e.g. Dr, Miss, Mr, Mrs, Ms)	
First Name	
Last Name	
Relationship to the Subject	
Postal Address (if different to subject's)	
Telephone number	
Mobile number	

How we will contact you

If you have made the request electronically (email) we will reply using that email address	Please confirm email address here:
If you have made the request in writing, please provide the postal address you want the response to be sent to:	Postal address:

Subject Access Request

Please provide specific details of your subject access request and the information you want:

Please send this form to:

If **electronically**, please email to **dpo@amwell.herts.sch.uk**
If by **post**, please send to **Data Protection Officer** **Amwell View School** **Station Road** **Stanstead Abbotts** **Hertfordshire. SG12 8EH**

15. Appendix 2

Data Breach Procedure

Policy Statement

Amwell View 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 procedure applies to all personal and sensitive data held by Amwell View School. This procedure applies to all school staff including governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Amwell View 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 personal data records concerned;
    b. communicate the name and contact details of the data protection officer 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.

Types of Breach

Data protection breaches could be caused by 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-attach;
- Hacking

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Headteacher and/or 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 (or nominated representative) 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 an IT technician.
3. The Headteacher/DPO (or nominated representative) 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 (or nominated representative) 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 (or nominated representative) 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 County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phising') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an appropriate 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 (or nominated representative).
    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 any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Headteacher/DPO (or nominated representative) to fully investigate the breach. The Headteacher/DPO (or nominated representative) 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 requirement to the 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 has been resolved.

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 (or nominated representative) should, after seeking expert or 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 individuals, 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 (School's Complaint Policy). 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.

Review and Evaluation

Once the initial aftermath of the breach is over, the Headteacher/DPO (or nominated representative) 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 and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the person leading the investigation should liaise with Human Resources 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.

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 Headteacher.

16. Appendix 2

DATA BREACH
REPORT FORM

Name……. Signature

Date

The **nature** of the personal data breach – in clear and plain language

A description of the likely **consequences** of the personal data breach

A description of the **measures taken**, or propose to take, to deal with the personal data breach and including, where appropriate, the measures taken to mitigate any personal adverse effects

Under GDPR, notification of certain data breaches will be compulsory by the DPO to the ICO (Information Commissioner's Office) within 72 hours of the breach, therefore it is important that staff report a Data Breach as soon as possible.
Please email this form to : **dpo@amwell.herts.sch.uk** immediately you suspect a data breach has occurred.