



## Data Protection Policy

**Last Reviewed Date:** 14/11/2016

<b>Headteacher:</b>		<b>Date:</b>	03/05/2018
<b>Chair of Governors:</b>		<b>Date:</b>	03/05/2018

**Date of Next Review:** May 2019

**C O N T E N T S**

<b>1</b>	<b>General Statement</b>
<b>2</b>	<b>Enquiries</b>
<b>3</b>	<b>Fair Obtaining and Processing</b>
<b>4</b>	<b>Lawful Basis</b>
<b>5</b>	<b>Data Integrity</b>
<b>6</b>	<b>Subject Access</b>
<b>7</b>	<b>Processing Subject Access Requests</b>
<b>8</b>	<b>Authorised Disclosures</b>
<b>9</b>	<b>Data and Computer Security</b>
<b>10</b>	<b>Physical Security</b>
<b>11</b>	<b>Software Security</b>
<b>12</b>	<b>Procedural Security</b>
<b>13</b>	<b>Appendix 1: Subject Access Request Form</b>



## 1. General Statement

This policy has been written to implement the new elements of data protection associated with the General Data Protection Regulation (GDPR) and associated Data Protection Bill which will replace Data protection Act 1998.

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Headteacher and Governors of this School intend to comply fully with the requirements and principles of the General Data Protection Regulation (GDPR) and associated Data Protection Bill which will replace Data protection Act 1998. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

## 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](mailto: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 and Specialist Sports College 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 Retention Policy is based on the IRMS Information Management Toolkit for Schools Version 5 (February, 2016). 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 and Specialist Sports College 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.

## 11. Physical 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. Appendix 1

# SUBJECT ACCESS REQUEST FORM

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

## 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 <b>electronically</b> , please email to <a href="mailto:dpo@amwell.herts.sch.uk">dpo@amwell.herts.sch.uk</a>
If by <b>post</b> , please send to  <b>Data Protection Officer Amwell View School and Specialist Sports College Station Road Stanstead Abbots Hertfordshire. SG12 8EH</b>