



## Data Protection Policy

### 1. Rationale:

The school needs to collect and to use specific personal information about a range of stakeholders. These include pupils, employees (current, past and prospective) and suppliers. This personal information must be dealt with appropriately and securely whether it is collected, stored or used electronically, on paper or in some other form. The Data Protection Act 1998 contains safeguards to ensure that personal data is handled correctly.

### 2. Definitions:

For this policy and in the Data Protection Act 1998 the following definitions apply

- 'Personal data' means information which relates to a living individual who can be identified. (Addresses and telephone numbers are particularly vulnerable to abuse but so too is a wider range of information, including names and photographs.)
- 'Processing' means obtaining, recording or holding the information or data or carrying out any set of operations on the information or data.
- 'Data subject' means or the person to whom the information relates.
- 'Parent' has the meaning given in the Education Act 1996 and the Children Act 1989 and includes any person having parental responsibility or care of a child.

### 3. Aims and Objectives:

The Data Protection principles, detailed in Schedule 1 of the Data Protection Act 1998, state that personal information

- Must be fairly and lawfully processed.
- Must be processed for specific purposes and not for any other reason incompatible with that purpose or those purposes.
- Shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
- Shall be accurate and, where necessary, kept up to date.
- Shall not be kept for longer than is necessary for the given purposes.

And that

- Appropriate technical and organisational measures shall be taken to prevent unauthorised or unlawful processing of data and to guard against accidental loss of, or damage to, personal data.
- Personal data shall not be transferred to another country or territory unless that country or territory ensures an adequate level of data protection.

### 4. Implementation:

The implementation of this policy covers a number of areas:



## Fair Obtaining and Processing

The 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.

## Registered Purposes

The Data Protection Registration entries for the School are available for inspection, by appointment, at the school. Explanation of any codes and categories entered is available from the 'Data Controller' who is the person nominated to deal with data protection issues in the School. Registered purposes covering the data held at the school are listed on the school's registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

## Data Integrity

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

- Data Accuracy
- Data Adequacy and Relevance
- Length of Time

*(For further information please see Appendix A: Ensuring Data Integrity.)*

## Subject Access

The Data Protection Acts extend to all data subjects 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 request for subject access is received from a pupil, the school's policy is that this will be processed and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request. In such cases 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.

*(For further information please see Appendix B: Processing Subject Access Requests.)*

## Authorised Disclosures

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

*(For further information please see Appendix C: Authorised Disclosures.)*

## Data and Computer Security

The school undertakes to ensure security of personal data by the following general methods (precise details cannot be given for security reasons):

- Physical Security
- Logical Security
- Procedural Security



The overall security policy for data is determined by the Principal and the Governing Body and is monitored and reviewed regularly. An automatic review will also be instigated if a security loophole or 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 Principal.

*(For further information please see Appendix D: Data and Computer Security.)*

## **5. Monitoring and Evaluation:**

- This policy will be reviewed regularly by the Governing Body through the appropriate committee.
- An internal review of the key areas listed in the 'Implementation' section above will be undertaken annually by the Strategic Leadership Team.
- Details of Data Subject Access requests will be entered in the 'Data Subject Access' logbook. A summary will be provided to the Principal on a termly basis and to Governors annually.
- Staff training will be organised, and individual participation recorded, by the Professional Development Coordinator.

## **6. Links:**

General/ further information about the Data Protection Act 1998 can be obtained from the Information Commissioner's Office, website [www.ico.gov.uk](http://www.ico.gov.uk)

## **7. Responsibilities:**

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. This responsibility is delegated to the Principal (registered with the Information Commissioner's Office as the 'Data Controller') who will ensure that all staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines. 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 a disciplinary matter, and serious breaches could lead to dismissal.

**8. Date of Approval by Governors:** 5<sup>th</sup> October 2016

**9. Next Review Date:** 5<sup>th</sup> October 2018



## **Appendix A: Ensuring Data Integrity**

### 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. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments. 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.

### Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Data Controller (or his/ her delegated colleague) to ensure that obsolete data are properly erased.

## **Appendix B: Processing Subject Access Requests**

Requests for access must be made in writing. Pupils, parents or staff may ask for a Data Subject Access Form (final Appendix to this document), also available from the School Office and our website ([www.penkethhigh.com](http://www.penkethhigh.com)). The completed form should be submitted to the Principal who will arrange for it to be processed. Provided that there is sufficient information to process the request, 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 the date on which sufficient information has been provided. In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

## **Appendix C: Authorised Disclosures**

The circumstances where the school's authorised officer may need to disclose data without explicit consent 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.
- 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 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.

## Appendix D: Data and Computer Security

### Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. 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.

### Logical 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 regularly.

### 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.



## Appendix E: Data Subject Access Form

### DATA PROTECTION ACT 1998 Section 7.

*Please print this form (or contact the school for a copy), complete in writing and send to the Principal.*

Enquirer's Surname \_\_\_\_\_

Enquirer's Forename(s) \_\_\_\_\_

Enquirer's Address \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Enquirer's Postcode \_\_\_\_\_

Telephone Number(s) \_\_\_\_\_

Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")? YES / NO

If 'NO',

Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about? YES / NO

If 'YES',

Name of child or children about whose personal data records you are enquiring

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested

# Penketh High School Policy



Additional information.

Please send reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

## DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Dispatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

\_\_\_\_\_

Name of "Data Subject" (or Subject's Parent) (PRINTED)

\_\_\_\_\_

Date

\_\_\_\_\_