



THE STONEHENGE SCHOOL

Data Protection Policy

General Statement

The Stonehenge School fully endorse and adhere to the principles of data protection as outlined in the Data Protection Acts 1994 and 1998. All staff involved in the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Enquiries

Information about The Stonehenge School Data Protection policy can be obtained from the school website.

Fair Obtaining and Processing

The Stonehenge 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 data is 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 the data will explain the issues before collection the information.

Terms

processing Obtaining , recording or holding the information or data or carrying out a set of operations on the information or data.

data subject means an individual who is the subject of personal data or the person to whom the data relates.

personal data means data which relates to a living individual who can be identified.

Addresses and telephone numbers are examples.

parent refers to the meaning given in the Education Act 1996, and includes any person who has parental responsibility for a child.

Registered Purposes

The Data Protection Act Registration entries for The Stonehenge School are available for inspection by appointment at The Stonehenge School. Explanation of any codes and categories is available from the Data Controller who is the person nominated to deal with data protection issues. 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 Stonehenge School undertakes to ensure that data integrity is achieved by the following methods:

- **Data Accuracy**

Data 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 any data subjects every twelve months so they can check its accuracy and make any amendments. Where a subject challenges the accuracy of their data, The Stonehenge School will immediately mark the record as potentially inaccurate. In cases of dispute, we will attempt to resolve the issue informally, but if this proves impossible, disputes will be referred to a senior management for their judgement. If the dispute cannot be resolved at this stage, either side may see independent arbitration. Until resolved, the information will be marked and both versions will be saved.

- **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 held. In order to ensure compliance with this principle, The Stonehenge School will check records regularly for missing, irrelevant or seemingly excessive information and may contact the 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 to ensure that obsolete data are properly erased.

- **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:

- Requests from pupils will be processed as any subject access request as outlined below 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.
- 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.



• **Processing Subject Access Requests**

Requests for access must be made in writing.

Learners, parents or staff may ask for a Data Subject Access form, available from the School Office. Completed forms should be submitted to the Data Controller. 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 (e.g. 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.

• **Authorised Disclosures**

The Stonehenge School will, in general, only disclose data about individuals with their consent. However there are circumstances under which The Stonehenge School authorised officer 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 the vicinity of the school.
- Staff data disclosed to relevant authorities e.g. 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. We 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 organisation, 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 organisation's registered purposes.



Data and Computer Security

The Stonehenge School undertakes to ensure security of personal data by the following general methods (precise details cannot be revealed):

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 (i.e. security copies are taken) 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.

Overall security policy for data is determined by the governing body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The Stonehenge School 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 Controller.

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.

Adopted by Governors