



DATA PROTECTION POLICY STATEMENT

The College will comply with:

- The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.
- Information and guidance displayed on the Information Commissioner's website (www.ico.gov.uk)
- This policy should be used in conjunction with the school's ICT Acceptable Use Policy.

About the Act

The Data Protection Act 1998 regulates the use of personal data. The College holds information on pupils in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the College as a whole is doing. This information includes contact details, assessment data, reports data, attendance information, special educational needs and any relevant medical information. Holding such information means that the College must abide by the Data Protection Act. This means, among other things, that the data held about pupils must only be used for specific purposes allowed by law.

Data protection law reinforces common sense rules of information handling, which most organisations try to follow anyway. It is there to ensure that organisations manage the personal information they hold in a sensible way. Organisations must keep the information accurate and up to date, they must only keep it for as long as they need it for a specified purpose and they must keep it secure.

Pupils, as data subjects, have rights under the Data Protection Act, including a general right of access to personal data held on them, with parents able to exercise this right on their behalf if they are too young to do so themselves. All rights under the Data Protection Act to do with information about a child, rest with that child, as soon as they are old enough to understand these rights. This will vary from one child to another. As a broad guide, it is reckoned that most children will have a sufficient understanding by the age of 12.

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.

Data Gathering

- All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.
- Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

Data Storage

- Personal data will be stored in a secure and safe manner.
- Electronic data will be protected by standard password and firewall systems operated by the College.

- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.
- Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
- Particular attention will be paid to the need for security of sensitive personal data.

Data and Computer Security

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

- Appropriate building security measures are in place, such as alarms, window bars and deadlocks.
- 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.
- 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.

Data Disclosures

- Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.
- When requests to disclose personal data are received by telephone it is the responsibility of the College to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back to ensure the possibility of fraud is minimised.
- If a personal request is made for personal data to be disclosed it is again the responsibility of the College to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.
- Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
- A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

Subject Access Requests

- If the College receives a written request from a data subject to see any or all personal data that the College holds about them this should be treated as a Subject Access Request and the College will respond within the 40 day deadline.
- Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the College will comply with its duty to respond within the 40 day time limit.
- This policy will be included in the Staff Handbook.
- Data Protection statements will be included on any forms that are used to collect personal data.