DATA PROTECTION POLICY

Committee:	Teaching and Learning and Community
Approved by FGB:	7 May 2013
Reviewed:	3 years
Date of next review:	May 2018
Responsible Officer:	Josephine Jenkins
Version:	2

1. The school will comply with:

   1.1 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.

   1.2 Information and guidance displayed on the Information Commissioner's website (https://www.gov.uk/data-protection/the-data-protection-act)

2. Data Gathering

   2.1 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.

   2.2 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.

3. Data Storage

   3.1 Personal data will be stored in a secure and safe manner.

   3.2 Electronic data will be protected by standard password and firewall systems operated by the school.

   3.3 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.

   3.4 Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data.

   3.5 Particular attention will be paid to the need for security of sensitive personal data.

4. Data Checking

   4.1 The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.

   4.2 Any errors discovered would be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

5. Data Disclosures

   5.1 Personal data will only be disclosed to organizations or individuals for whom consent has been given to receive the data, or organizations that have a legal right to receive the data without consent being given.

   5.2 When requests to disclose personal data are received by telephone it is the responsibility of the school 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, preferably via a switchboard, to ensure the possibility of fraud is minimized.

5.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the school 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.

5.4 Personal data will only be disclosed to Police Officers if they are able to show a legitimate need to have access to specific personal data.

5.5 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.

6. Subject Access Requests

6.1 If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a subject Access Request and the school will respond within the 40 day deadline.

6.2 Informal requests to view or have copies or 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 school will comply with its duty to respond within the 40 day time limit.

7. Data protection statements will be included in the school prospectus and on any forms that are used to collect personal data.

8. The Data Protection coordinator is the school's HR officer.

Appendix 1

There are 8 Principles of Data Protection

1. Personnel data must be obtained and processed Fairly and Lawfully
2. Personal Data must only be held and processed for limited purposes
3. Data held must be adequate, relevant and not excessive in relation to the purposes for which it is held
4. Data must be accurate, and up to date
5. Data must not be held for longer than is necessary for the registered purpose
6. Data must be held and processed in accordance with the data subject's right
7. Data must be protected by appropriate technical and organisational security measures
8. Data must only be transferred to Countries within the EEA or those with adequate levels of data protection