

Data Protection Policy

Aim and introduction

1. This policy sets out how Chapelton Academy deals with personal information correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation.
2. This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.
3. All school staff and governors involved with the collection, use, processing or disclosure of personal data will be made aware of their duties and responsibilities and will adhere to this policy.
4. The Academy collects and uses personal information (referred to in the Data Protection Act as personal data) about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.
5. Prior to the signing of its Funding Agreement, the Academy will register as a Data Controller, with the Information Commissioner's Office (ICO). Details will be available on the ICO website.
6. The Academy issues a Privacy Notice to all students/parents; this summarises the information held on pupils, why it is held and the other organisations to whom it may be passed.

What is Personal Information/ data?

7. Personal information or data is information which relates to a living individual who can be identified from that data, or from that data in addition to other information available to them. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Data Protection Principles

8. The Data Protection Act 1998 establishes eight principles that must be adhered to at all times
 - a. Personal data shall be processed fairly and lawfully;
 - b. Personal data shall be obtained only for one or more specified and lawful purposes;
 - c. Personal data shall be adequate, relevant and not excessive;

- d. Personal data shall be accurate and where necessary, kept up to date;
- e. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
- f. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
- g. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
- h. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Implementing the Principles

9. The Academy is committed to maintaining the above principles at all times. Therefore the Academy will:
- a. Inform individuals why personal information is being collected.
 - b. Inform individuals when their information is shared, and why and with whom unless the Data Protection Act provides a reason not to do this.
 - c. Check the accuracy of the information it holds and review it at regular intervals.
 - d. Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
 - e. Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
 - f. Ensure that personal information is not retained longer than it is needed.
 - g. Ensure that when information is destroyed that it is done so appropriately and securely.
 - h. Share personal information with others only when it is legally appropriate to do so.
 - i. Comply with the duty to respond to requests for access to personal information, known as Subject Access Requests.
 - j. Ensure that personal information is not transferred outside the EEA without the appropriate safeguards.
 - k. Ensure all staff and governors are aware of and understand these policies and procedures.

Responsibilities

- 10. The Governing Body is responsible for** ensuring that all staff are given appropriate training so that they understand their role and responsibilities in relation to data protection.
- 11. The Finance, Business and HR Manager is responsible for** all other operational aspects of compliance with data protection legislation.

Complaints

12. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Monitoring and Review

13. The FBM will report on the Academy's performance in relation to data protection. The report will be sent annually to the Governing Body, in conjunction with the SAR. The Governing Body will make recommendations based on this report and the data it contains.

Signed by *R Maxted & ADexter*

Agreed by TGB **March 2014**

Reviewed by	Temporary Governing Body
Last Reviewed	February 2016
Adopted by GB	May 2016
Next Review	Academic Year 2017/2018