Data Protection Policy

January 2017

Next Review Due: January 2018

Co-ordinator: Miss M Newton/Mrs J McColl

ACADEMY DATA PROTECTION POLICY	
POLICY DATE: JANUARY 2017	**REVIEW DATE: JANUARY 2018**

Introduction

The Academy is required to maintain certain personal data about living individuals for the purposes of satisfying operational and legal obligations. The Academy recognises the importance of the correct and lawful treatment of personal data; it maintains confidence in the organisation and provides for successful operations.

The types of personal data that the Academy may require include information about: current, past and prospective employees; pupils; suppliers and others with whom it communicates. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

The Academy fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for the Academy must adhere to these principles.

Principles

The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
3. Be adequate, relevant and not excessive for those purposes;
4. Be accurate and, where necessary, kept up to date;
5. Not be kept for longer than is necessary for that purpose;
6. Be processed in accordance with the data subject's rights;
7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures;
8. And not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Satisfaction of principles

In order to meet the requirements of the principles, the Academy will:

- observe fully the conditions regarding the fair collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- ensure the quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act;

- take the appropriate technical and organisational security measures to safeguard personal data;

The Academy's Designated Data Controller
The Academy's Office Manager is responsible for ensuring compliance with the Data Protection Act and implementation of this policy.

Status of the policy
This policy has been approved by the Governors and any breach will be taken seriously and may result in formal action.

Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Office Manager or the Headteacher.

Subject access
All individuals who are the subject of personal data held by the Academy are entitled to:

- Ask what information the Academy holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what the Academy is doing to comply with its obligations under the 1998 Data Protection Act.

Employee responsibilities
All employees are responsible for:

- Checking that any personal data that they provide to the Academy is accurate and up to date.
- Informing the Academy of any changes to information which they have provided, e.g. changes of address.
- Checking any information that the Academy may send out from time to time, giving details of information that is being kept and processed.
  If, as part of their responsibilities, employees collect information about other people (e.g. personal circumstances, or about employees), they must comply with the Policy and with the Data Protection Procedures.

Data security
The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Rights to access information
Employees, pupils and other subjects of personal data held by the Academy have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. This right is subject to certain exemptions which are set out in the Data Protection Act. Any person who wishes to exercise this right should make the request in writing to the Headteacher.
The Academy reserves the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they can be amended upon request.
The Academy aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a written request unless

there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

Publication of Academy information
Information that is already in the public domain is exempt from the 1998 Act. This would include, for example, information on staff contained within externally circulated publications such as the Academy Prospectus. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Headteacher.

Subject consent
The need to process data for normal purposes has been communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained. Processing may be necessary to operate Academy policies, such as health and safety and equal opportunities.

Retention of data
The Academy will keep some forms of information for longer than others. All staff are responsible for ensuring that information is not kept for longer than necessary.

Data protection code of practice

1. **Introduction**
   This Code of Practice must be read in conjunction with the Academy's Data Protection Policy document to give the fullest picture of its data protection regime. This document gives an introduction to some basic points of practice relating to the handling and processing of personal data.

2. **Key Concepts**
   The Data Protection Act 1998 places an obligation upon the Academy, as a data controller, to collect and use personal data in a responsible and accountable fashion. The Academy is committed to ensuring that every current employee and registered pupil complies with this Act to ensure the confidentiality of any personal data held by the Academy in whatever medium. Three key concepts to be considered are those of purpose, fairness and transparency.

3. **Purpose**
   Data controllers can only process personal data where they have a clear purpose for doing so and then only as necessitated by that purpose. Paragraphs 39–50 of this Code of Practice summarise the purposes for which the Academy processes personal data. Personal data cannot be processed for purposes that have not been defined and declared by the Academy.

4. **Fairness**
   In defining the purposes for which the Academy processes personal data, the fairness of that processing must be considered. For some types of processing the required elements of fairness and legality are clearly outlined in the legislation. Transparency Members of staff, students and others must be able to feel that there is no intention to hide from them details of how their personal data are collected, used and distributed by the Academy. One of the functions of this Code of Practice is to provide that assurance.

Collection and Amendment of Personal Data

Collection of personal data
In most cases, the personal data held by the Academy will be obtained directly from the data subjects themselves. The law stipulates that a data protection notice must accompany any request for personal data. Any members of staff responsible for managing the collection of personal data for the legitimate activities of the Academy must ensure that a notice containing the following information is included in the request for that data:

- A statement that the Academy is the data controller
- The name and or job title of the specific member of staff responsible for the administration of the

- personal data being collected, to enable, for example, subsequent amendments to be submitted by the data subject
- A clear explanation of the types of data being collected and the purposes for which that data will be processed
- Any further information that is considered necessary to ensure that the data processing can be described as being fair, for example details of any third parties to whom the data might be disclosed
- A statement making it clear that by submitting the personal data, the data subjects are giving their consent for the processing of the data for the stated purposes to take place.

Amendment of personal data

From time to time data subjects will wish to update some of their personal data held by the Academy, for example their home addresses or other contact details previously submitted. To do this, the data subjects must either contact the specific member of staff designated in the data protection notice at the time the data was submitted.

Security of personal data

. Of fundamental importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside the Academy. Authorised disclosures or transfers are those that are defined within the appropriate Notifications and declared to the data subject either at the point of data collection or subsequently, the necessary consent for disclosure or transfer having been obtained if required. To help ensure the security of personal data within the Academy, all those who process such data in the course of performing their duties are required to follow the general guidelines set out below.

Secure storage of personal data

Each member of staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage, in line with the Data Protection Policy, which states that personal data should:

Be kept in a locked filing cabinet, drawer, or safe; or if it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Ordinarily, personal data should never be stored at staff members' homes, whether in
. manual or electronic form, on laptop computers or other personal portable devices or at other remote sites**.**

Staff should be aware that log files would record details of all users who access, alter or
. delete or attempt to access, alter or delete centrally held computerised databases and files containing personal data.

. **Secure processing of personal data**

While staff members in the course of performing their legitimate duties are using personal data, reasonable precautions must be taken to ensure the safety and privacy of that data. For example:

- In open-plan offices, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised staff may

readily see that data, and password- protected screensavers should be used.

- Personal data in manual form, such as in paper files, correspondence or database printouts, should not be left in view in open-plan offices while the relevant staff members are away from their desks. They should instead be locked away or at least covered.
- Where manual records containing personal data are accessible to a number of staff in
  the course of their legitimate activities, access logbooks should be used where practicable
  to help monitor the whereabouts and use of such records.

. Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Headteacher must be obtained, and all the security guidelines given in this document must still be followed.

The disclosure and transfer of personal data

Publication of Academy Information

While the majority of personal data held by the Academy is processed for internal administrative purposes and is never disclosed outside the institution, some categories of data are routinely or from time to time released through one or more forms of publication.

Legal obligations

When required by law or Academy statute, the names of staff and Governors of the Academy and certain other personal data relating to employees and Governors are published in the annual certain documents and on the Web site. The Academy also fulfils all obligations placed upon it by its relationship with various funding bodies, Government Agencies and the like with regard to the release of personal data and statistical information concerning pupils and staff. Data subjects are informed of the Academy's obligations in this respect.

Staff Directory
In order to meet the legitimate needs of researchers, visitors and enquirers to be able to make contact with appropriate staff, the Academy has available on its public Web site a list of staff members, the office telephone number and office e-mail address.

Pupil personal data on Web pages
Apart from the obligations mentioned above the Academy will not ordinarily reveal any personal details of pupils enrolled at the Academy to any individual or body outside the Academy.

The Academy has a duty to retain some staff and pupil personal data for a period of time following their departure from the Academy, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, or example relating to pensions and taxation. Different categories of data will be retained for different periods of time.

The disposal of personal data
When a record containing personal data is to be disposed of, the following procedures will be followed:

All paper or microfilm documentation containing personal data will be permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data.
All computer equipment or media that are to be sold or scrapped will have had all personal data completely destroyed, by re-formatting, over-writing or degaussing.

Employees and, where appropriate, pupils, will be provided with guidance as to the correct mechanisms for disposal of different types of personal data and audits will be carried out to ensure that this guidance is adhered to. In particular, employees will be made aware that erasing/deleting electronic files does not equate to destroying them.