



# **Data Protection Policy**

## **June 2016**

## **Aims & Objectives**

The aim of this policy is to provide a set of guidelines to enable staff, parents and pupils to understand:

- The law regarding personal data
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and pupils can access personal data

The objective of the policy is to ensure that the school acts within the requirements of the Data Protection Act 1998 when retaining and storing personal data, and when making it available to individuals, and that the process of responding to enquiries for other information is also legal under the Freedom of Information Act 2000 (in force from 1<sup>st</sup> January 2005).

## **Definitions**

'The Trust' refers to overarching responsibilities of The Spencer Academies Trust.

'The Academy' refers to the individual responsibilities of each member Academy.

'Academies' refers to the responsibilities of every member Academy within the Trust

## **Policy Statement**

The Spencer Academies Trust is committed to a policy of protecting the rights and privacy of individuals (includes students, staff and others) in accordance with the Data Protection Act 1998 (the Act). The Trust and Academies need to process certain information about staff, students and other individuals that they have dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff and students of the Trust. Any breach of the Data Protection Act 1998 or the Trust Data Protection Policy will be taken seriously and may result in disciplinary action. As a matter of good practice, other agencies and individuals working with the Academies, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

## **Background to the Data Protection Act 1998**

The Data Protection Act 1998 enhances and broadens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

## **Responsibilities under the Data Protection Act**

The Trust, as a body is the data controller under the Act. A Data Protection Officer has been appointed who is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for data users in the Academies

The Trust Executive Team, and all those in managerial or supervisory roles are responsible

for developing and encouraging good information handling practice within the Academies.

Compliance with data protection legislation is the responsibility of all individuals within the Academies who process personal information.

Data processors are responsible for ensuring that any personal data supplied to the Academy are accurate and up-to-date. Notification is the responsibility of the Registrar and the Data Protection Officer. Details of the Trust's notification are published on the Information Commissioner's website. Anyone who is, or intends, processing data for purposes not included in the Trust's Notification should seek advice from the Data Protection Officer.

### **Data Protection Terms**

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal or school report).

Data controllers are the people or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our Academies.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf such as suppliers who provide payroll services for us.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data

can only be processed under strict conditions, and will usually require the express consent of the person concerned.

### **Data Protection Principles**

All processing of personal data must be done in accordance with the eight data protection principles.

1. Personal data shall be processed fairly and lawfully. Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes. Data obtained for specified purposes must not be used for a purpose that differs from those without notice being provided to the data subject.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held. Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.
4. Personal data shall be accurate and, where necessary, kept up to date. Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of all data users to ensure that data held is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate. Individuals should notify the Academy of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Academy to ensure that any notification regarding change of circumstances is noted and acted upon.
5. Personal data shall be kept only for as long as necessary. This means that data should be destroyed or erased from our systems when it is no longer required.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.
8. Personal data must not be transferred outside of the European Economic Area (EEA) - the fifteen EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. [Data processors should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.]

## **Data Subject Rights**

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision making process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

## **Consent**

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The Academy understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by the Academy (e.g. when a student signs a registration form or when a new member of staff signs a contract of employment). Any Academy forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.

If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any member of the Academy is in any doubt about these matters, they should consult the Trust Data Protection Officer.

## **Security of Data**

All Academy staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. You should form a judgment based upon the sensitivity and value of the information in question, but always consider keeping personal data in a lockable room with controlled access, or in a locked drawer or filing cabinet, or if computerised, password protected, or kept on media which are themselves kept securely.

Care should be taken to ensure that Computer screens are not visible except to authorised staff and that passwords are kept confidential. Screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant computers should be wiped clean before disposal.

This policy also applies to staff and students who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside of the Academy.

### **Rights of Access to Data**

Data subjects have the right to access any personal data which are held by any Academy in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Academy about that person.

Any individual who wishes to exercise this right should apply in writing to the Trust Data Protection Officer or the Company Secretary. The Trust reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

Any member of staff who receives a written request should forward it to the Trust Data Protection Officer or the Company Secretary.

### **Disclosure of Data**

The Academies must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of Academy business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the Academy concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions applies: []C the individual has given their consent (e.g. a student/member of staff has consented to the Academy corresponding with a named third party);

- where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other Academy employees if it is clear that those members of staff require the information to enable them to perform their jobs);
- where the institution is legally obliged to disclose the data (e.g. ethnic minority and disability monitoring);
- where disclosure of data is required for the performance of a contract (e.g. informing a student's LEA or sponsor of course changes/withdrawal etc.). The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:
- to safeguard national security\*; prevention or detection of crime including the apprehension or prosecution of offenders\*; assessment or collection of tax duty\*; discharge of regulatory functions (includes health, safety and welfare of persons at work)\*; to prevent serious harm to a third party; []C to protect the vital interests of the individual, this refers to life and death situations. \* Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member of the Academy, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the Academy may constitute an unauthorised disclosure. Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request. As an alternative to disclosing personal data, the Academy may offer to do one of the following:

- pass a message to the data subject asking them to contact the enquirer;
- accept a sealed envelope/incoming email message and attempt to forward it to the data subject. Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the Academy" to avoid confirming their membership of, their presence in or their absence from the institution.

### **Retention and Disposal of Data**

The Academy discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and students. However, once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

**Students** - In general, electronic student records containing information about individual students are kept indefinitely and information would typically include name and address on entry and completion, programmes taken, examination results, awards obtained.

**Staff** - In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address,

positions held, leaving salary. Other information relating to individual members of staff will be kept by the Personnel Department for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc. will be retained for the statutory time period (between 3 and 6 years).

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, been short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

### **Disposal of Records**

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion). Publication of Academy Information. It should be noted that the Trust publishes a number of items that include personal data, and will continue to do so. These personal data are:

Information published in the Academy Calendar including: names of all members of Trust and Academy Committees Names, job titles and academic and/or professional qualifications of members of staff. Internal Telephone Directory. Information in prospectuses (including photographs), annual reports, staff newsletters, etc. Staff information on the Academy website (including photographs).

It is recognised that there might be occasions when a member of staff, a student, or a lay member of the Academy, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the Academy should comply with the request and ensure that appropriate action is taken.

### **Use of CCTV**

The Trust's use of CCTV is regulated by a separate Code of Practice.

For reasons of personal security and to protect Academy premises and the property of staff and students, close circuit television cameras are in operation in certain locations. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- any monitoring will be carried out only by a limited number of specified staff; personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete; staff involved in monitoring will maintain confidentiality in respect of personal data.

### **Monitoring and review of the policy**

This policy is reviewed bi-annually, or in the event of a significant change of relevant guidance, by the Trust Executive Leadership team. The Trust will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.