KING EDWARD VI
SHELDON HEATH ACADEMY

DATA PROTECTION POLICY

1. Policy Statement

KESH Academy ("the Academy") 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. The Academy needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes (e.g. to recruit staff, to administer programmes of study, to record progress, 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 Academy. Any breach of the Data Protection Act 1998 or the Academy Data Protection Policy may be considered to be a disciplinary offence and in that event, Academy disciplinary procedures will apply.

2. 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.

3. Definitions (Data Protection Act 1998)

Personal Data
Personal data includes information that relates to a living person. It is information that identifies an individual either on its own or together with other information that is in the organisation's possession currently or in the future.

Sensitive Data
Different from ordinary personal data (such as name, address, telephone number) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller
Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject
Any living individual who is the subject of personal data held by an organisation.

Processing
Any operation related to organisation, retrieval, disclosure and deletion of data and includes: obtaining and recording data, accessing, altering, adding to, merging, deleting data, retrieval, consultation or use of data, disclosure or otherwise making available of data.

Third Party
Any individual/organisation other than the data subject or the data controller.

Relevant Filing System
Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

4. Responsibilities under the Data Protection Act

- The Academy as a body corporate is the data controller under the new Act.
- A Data Protection Officer is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for members of the Academy. The Data Protection Officer is currently the Director of Finance and Resources.
- The Leadership team and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the Academy.
- Compliance with data protection legislation is the responsibility of all members of the Academy who process personal information.
- Members of the Academy are responsible for ensuring that any personal data supplied are accurate and up-to-date.

5. Training and awareness

- The Academy will ensure that all staff are made aware of good practice in data protection. It will do this by providing adequate training for all staff responsible for personal data and will include awareness training as part of the staff induction process.
- The Academy will ensure that everyone handling personal data knows that they should refer issues to the Director of Finance and Resources in order to obtain further guidance.

6. 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.
2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data shall be kept only for as long as necessary.
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 shall not be transferred to a country or a 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.

7. Notification and Data Collection

The Information Commissioner's Office maintains a public register of data controllers. Each register entry includes the name and address of the data controller and details about the types of personal information they process. Individuals can check the register to find out what processing of personal information is being done by a particular data controller. Notification is the process by which a data controller's details are added to the register.

All Data Controllers have to consider whether they are exempt from Notification. If they are not exempt, they have to Notify. This means completing a form for the Information Commissioner, and paying a fee each year. The Notification form covers:

- The purposes for which personal data is held (from a standard list) and for each purpose (again from standard lists):
- The types of Data Subject about whom data is held
- The types of information that are held
- The types of disclosure that are made
- Any transfers abroad

It is the view of the KESH Academy, as the Data Controller, that it needs to Notify.

The Information Commissioner Registration entries for KESH Academy are available for inspection, by appointment, at the Academy. Explanation of any codes and categories entered is available from the Director of Finance and Resources. Registered purposes

covering the data held at the Academy are listed on the school's Registration and data collection documents.

Information held for these stated purposes will not be processed for any other purpose without the data subject's consent.

8. Data Storage and security

- The Academy will hold the minimum amount of personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed.
- The Academy will store personal data in a secure and safe manner.
- Electronic data will be protected by standard password and firewall systems operated by the Academy.
- Personal data, the loss of which could cause damage or distress to individuals, which is used or stored on portable or mobile devices will be encrypted using encryption software which meets the current standard or equivalent. This applies to all laptop computers and portable memory devices (including memory sticks etc)
- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers.
- Paper records will be managed so that access is restricted to those who need to use the information and stored in secure locations to prevent unauthorised access.
- Computer systems will be designed and computer files created with adequate security levels to preserve confidentiality. Those who use the Academy's computer equipment will have access only to the data that is both necessary for the work they are doing and held for carrying out that work.
- 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 PCs should be wiped clean before disposal.
- Particular attention will be paid to the need for security of sensitive personal data.

9. Data Checking

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

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

10. 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 member of staff taking the call 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 minimised.
- If a personal request is made for personal data to be disclosed it is again the responsibility of the member of staff 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.
- 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.
- Routine consent issues will be incorporated into the Academy's student data gathering sheets, to avoid the need for frequent, similar requests for consent being made.
- Personal data will only be disclosed to Police Officers if they are able to supply a relevant document which notifies of a specific, legitimate need to have access to specific personal data.
- A record will be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

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;
- to protect the vital interests of the individual, this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

11. Subject Access Requests

Subject access requests should be notified to the Data Protection Officer. If the Academy receives a written request from a data subject to see any or all personal data that the Academy holds about them this will be treated as a legitimate Subject Access Request and the Academy will respond within the recommended 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 Academy will comply with its duty to respond within the 40 day time limit.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity must be verified before handing over any information.

The Data Protection Registrar states that a fee per request can be charged and the Academy may do this at its discretion. When the subject access request is received and acknowledged the Data Protection Officer will inform the individual of the charge and seek confirmation that they still wish to make a subject access request.

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;
- to protect the vital interests of the individual, this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

12. 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, courses taken, examination results and awards obtained.

Staff
Information relating to individual members of staff will be kept by the HR Department in accordance with the retention guidelines published by the Records Management Society of Great Britain, Retention Guidelines for Schools.

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).

13. Use of CCTV

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 site 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 review of CCTV footage will be carried out only by a limited number of specified staff ("authorised CCTV operators");
- 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.

The release of the recorded images to third parties will be made only in accordance with the KESH CCTV policy.

This policy was approved by KESH Academy Finance Committee in March 2015. The policy is scheduled to be reviewed every two years unless the legislation changes.