HART SCHOOLS TRUST

DATA PROTECTION POLICY

Document produced by:	Mark Lewis
Date Adopted:	5 April 2017
Review date:	31 March 2019

POLICY STATEMENT

The Data Protection Act 1998 ("the Act") is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's *personal data*.

The Hart Schools Trust (HST) regards the lawful and correct treatment of personal information as essential to the successful and efficient performance of its functions, and to maintaining confidence between itself and those with whom it deals. To this end, HST fully endorses and adheres to the eight Data Protection Principles set out in the Act http://www.legislation.gov.uk/ukpga/1998/29/contents.

PURPOSE

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Awareness of this policy will help staff and members of HST understand the purpose and principles of Data Protection. In addition, it will contribute to ensuring that the Trust has guidelines and procedures in place which are consistently followed. Failure to adhere to the Act's requirements could result in legal action being taken against HST.

DEFINITIONS

"data controller" means the person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

"data subject" means an individual who is the subject of *personal data* or the person to whom the information relates.

"parent" has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

"personal data" means data which relates to a living individual who can be identified[1]

"processing" means obtaining, recording or holding *personal data* or carrying out any or set of operations on those data.

"sensitive personal data" means information about a child and any data which includes:

- The racial or ethnic origin of the *data subject*
- Political opinions
- Religious or other beliefs of a similar nature
- Membership of trade unions
- Physical or mental health or condition
- Sexual life
- Information concerning the commission of any offence or criminal records

[1] Addresses and telephone numbers are particularly vulnerable to abuse, but so are names and photographs or CCTV recordings, if published by whatever means.

SCOPE OF THE POLICY

Personal data is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to *personal data* held visually in photographs or video clips (including CCTV) or as sound recordings.

The Trust collects a large amount of *personal data* every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the Trust's schools. In addition, it may be required by law to collect and use certain types of information to meet the statutory obligations of Local Authorities (LAs), government agencies and other bodies.

DATA PROTECTION PRINCIPLES

The Act is based on eight data protection principles, or rules for 'good information handling':

1. Data must be processed fairly and lawfully.

2. *Personal data* can be obtained and held only for specific and lawful purposes.

3. *Personal data* being held should be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

4. *Personal data* shall be accurate and where necessary kept up to date.

5. *Personal data* processed for any purpose(s) should not be kept for longer than is necessary for that purpose.

6. *Personal data* should be processed in accordance with the rights of *data subjects* under the 1998 Data Protection Act.

7. Appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of *personal data* and against accidental loss or destruction of, or damage to, *personal data*.

8. *Personal data* must not be transferred to a country outside the EEA, 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*.

THE TRUST'S RESPONSIBILITIES

The Trust must:

- Manage and process *personal data* properly
- Protect individuals' right to privacy
- Provide an individual with access to all *personal data* held on them.

The Trust is committed to upholding the eight data protection principles and so will:

- inform *data subjects* why it needs *personal data*, how it will use such data and with whom it may be shared. This is done by providing a Privacy Notice or Fair Processing Notice.
- periodically check the quality and accuracy of the information held.

- apply the records management policies and procedures to ensure that information is not held longer than is necessary.
- ensure that when information is authorised for disposal it is done appropriately.
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system.
- only share personal information with others when it is necessary and legally appropriate to do so.
- set out clear procedures for responding to requests for access to personal information (known as subject access requests).
- train all staff so that they are aware of their responsibilities and of the schools relevant policies and procedures.

The HST has a legal responsibility to comply with the Act, and HST employees and members who process or use any personal information in the course of their duties must ensure that these principles are followed at all times. The HST, as a corporate body, is named the Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

The HST is required to 'notify' the Information Commissioner of the processing of *personal data*. This information will be included in a public register available on the Information Commissioner's website at the following link:
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

WHY WE COLLECT PERSONAL DATA AND HOW WE PROCESS IT

HST obtains *personal data* (names, addresses, phone numbers, email addresses and photographs) on application forms and references and in some cases other documents from staff, students, parents, governors and volunteers. This data is stored and processed for the following purposes:

- The admission, education and development of students, including monitoring progress, attainment, achievement, behaviour, health and welfare.
- The recruitment of staff.
- Equal Opportunities monitoring.
- To distribute relevant organisational material e.g. school newsletters, meeting papers.
- To permit the payment of staff and for services and the receipt of monies due.
- Educational monitoring and improvement.
- Marketing.

All post and email marked as Private, Personal and/or Confidential (or similarly described) will be opened by the addressee only.

The contact details of staff, students, parents, governors and volunteers will only made available to other staff and members and the Hart Learning Group Human Resources (HR)

department. Any other information supplied on application will be kept in a secure filing cabinet and is not accessed during the day-to-day running of the organisation.

Personal data held by the Trust will not be sold or given to any other organisation or business for marketing purposes.

Contact details of staff and members will not be passed on to anyone outside the HST and the North Hertfordshire College Human Resources (HR) department without their explicit consent unless there is a legal obligation to do so.

ACCURACY

HST will take reasonable steps to keep *personal data* up to date and accurate.

STORAGE AND RETENTION

The Act's principles require the Trust to store data securely and not to hold data for longer than is necessary. Once *personal data* is no longer required by the Trust, it will be disposed of securely in accordance with Data Protection principles.

All reasonable steps are taken to ensure that data is stored in organised and secure systems.

The following guidelines will be applied to the retention of *personal data:*

- *Personal data* relating to employees will be stored for seven complete tax years after an employee has ceased to work for the Trust.
- *Personal data* relating to students will be held until the end of the academic year in which the student would turn 25.

The Managing Director is responsible for arranging the secure destruction of personal data files.

INFORMATION SECURITY

When accessing confidential information, HST Electronic Storage Devices are encrypted before use and are only removed from site where absolutely necessary for the purpose of carrying out contractual duties.

SCANNING

Electronic Storage Devices are cleared immediately after use when used to scan confidential documents from the printer/copier.

USE OF PHOTOGRAPHS

HST seeks permission from individuals and parents before displaying photographs in which they appear. This policy also applies to photographs published on the organisation's websites, in HST Promotional Material or media press releases.

COMPLIANCE

All staff and volunteers, paid or unpaid, are responsible for maintaining compliance with the Act. HST will regard any breach of any provision of the Act as a serious matter which will result in disciplinary action and which may result in dismissal for gross misconduct.

Any questions or concerns about the interpretation or operation of this policy statement should first be referred to the line manager and then to the Data Protection Officer.

SUBJECT ACCESS REQUESTS

The Data Protection Act gives individuals the right to ask the Trust to provide copies of the personal information HST holds about them – the right of subject access (SAR). The definition of *personal data* for this purpose extends to any *personal data* held on record anywhere by the Trust in structured files and in educational records, not just that held electronically. It includes information in correspondence and in notes made by governors, teachers and other staff.

Parents can make SARs on their children's behalf if the children are deemed too young to look after their own affairs or they have consented to their parents doing this on their behalf.

The Trust must respond to SARs within **forty calendar days** of receiving the request either providing the information requested or explaining why it is not possible to do so.

Handling subject access requests can be difficult and time consuming. Getting it right is important, particularly if other individuals' *personal data* is included in the information that the requestor seeks. There are some exemptions to the right of access to information in certain records held by academies/schools. Therefore all SARs must be forwarded to the Data Protection Officer who is fully trained in all the legal provisions and the exemptions that apply to subject access requests.

Subject access rights under the DPA are separate to the right of access to educational records under the Pupil Information Regulations for England, Northern Ireland, Scotland and Wales, which give a parent the right to information in their child's educational record.

TRAINING

Staff will be made aware of the content of this policy as part of their induction to HST. When significant changes are proposed staff will be updated. The policy will be accessible to all staff.

COMPLAINTS

Complaints will be dealt with in line with the school's complaints policy. Complaints about information handling may be referred to the Information Commissioner (the statutory regulator).

REVIEW

This policy will be reviewed as often as necessary, but at least every two years.

CONTACT

Further information and guidance about Data Protection is available from the Office of the Information Commissioner (https://ico.org.uk/).

The Trust's Data Protection and FOI Officer is:

Robert Dale, Company Secretary and Clerk
E: rdale@nhc.ac.uk
T: 01462 443066