HEARTSACADEMYTRUST

Data Protection Policy

Adopted by Directors: May 2018
To be reviewed: October 2020

HEARTS Academy Trust is committed to providing a happy, caring and safe learning environment for all within a values led context, where everyone feels valued and grows in confidence and independence.

We promote **HAPPINESS** through a creative, exciting and practical curriculum, which generates a love of, and interest in, learning and a resilience and hope which supports us through challenging times.

Great value is placed on pupils' self **ESTEEM** which is developed through a positive and motivated attitude to learning, a healthy lifestyle, good social skills, self-discipline and a positive self-image.

We promote the highest standards of **ACHIEVEMENT** in all areas of the curriculum and help all pupils to fulfil their potential regardless of gender, race or ability.

We foster **RESPECT and RESPONSIBILITY** for all by establishing good relations between the school, home and community. Pupils are taught respect for themselves, others and the environment. They are also taught to take full responsibility for their own choices and responsibility for themselves and their community.

We encourage **TRUTH** and honesty in all aspects of school life – relationships, work and the curriculum and learn to trust and accept others' individuality and uniqueness.

We develop **SPIRITUALITY and SERVICE** so that calm, quiet, reflective times which support deep thought are part of school life and beauty is appreciated. We promote a service culture that reflects our duty to support and show compassion to all members of the community and not just ourselves.

Children at the HEART

This policy reflects the aims and principles of the Trust, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents, volunteers, LAB Members, Trustees and Members.

The HEARTS Academy Trust needs to keep certain information about its employees, pupils, parents, volunteers, third parties and Governance to monitor performance and achievement. It is also necessary to process information so that staff can be recruited and remunerated, and legal obligations to funding bodies and government complied with.

To comply with the law, information must have a legal or statutory basis for collection and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the HEARTS Academy Trust must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act), the GDPR 2018 and the proposed Data Protection Act 2018.

In summary these state that the Trust will be transparent, have stringent controls in place and be accountable for all data collected.

People have the following rights:

- To be informed
- To have information rectified
- To erasure
- To restrict processing
- To data portability

Data must at all times:

- Be obtained and processed fairly and lawfully
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for that purpose
- Be accurate and kept up to date
- Not be kept for longer than is necessary for that purpose (see records retention policy)
- Be processed in accordance with the data subject's rights
- Be kept safe from unauthorised access, accidental loss or destruction using strict electronic controls and safeguards and securely stored
- Will be mapped according to the GDPR
- Will only be shared in accordance with the Privacy Notices

The HEARTS Academy Trust and all staff who process or use personal information must ensure that they follow these principles at all times.

Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the code of conduct, rules and policies made by the Trust. Any failures to follow this policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers
The Trust as a body corporate is the Data Controller under the 1998 Act, and the Trustees are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The Head of School is the designated Data Controller in schools. The Trust Business Manager is the designated Data Controller for central staff.
Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller via the school/Trust office.

The Data Protection Officer and Deputy Data Protection Officer are responsible for training staff, monitoring compliance and implementing audits. The DPO and DDPO will not monitor compliance of their own responsibility area. Any breach of data must be reported to the DPO/DDPO immediately and a failure to this will be a disciplinary matter.

The DPO and DDPO monitor compliance with regular reviews which include the effectiveness of data handling, processing activities and security controls.

Responsibilities of Staff

All staff are responsible for:
• Checking that any information that they provide to the school/Trust in connection with their employment is accurate and up to date.
• Informing the school/Trust of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The school/Trust cannot be held responsible for any errors unless the staff member has informed the school/Trust of such changes.
- Keeping data safe
- Collecting data only when it is necessary and ensuring the safe disposal when it is no longer required

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a pupil's work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Trust's Data Protection Policy.

Data Security

All staff are responsible for ensuring that:
- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing, via Web pages, social media or by any other means, accidentally or otherwise, to any unauthorised third party. If there is any doubt, staff should refer to the Privacy Notices and the DPO/DDPO.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information 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 an encrypted removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe and not removed from the school site.
- Where the facility allows, office doors should be locked with a key or key-code

Subject Access Information

All staff, parents and other users are entitled to:
• Know what information the school holds and processes about them or their child and why.
• Know how to gain access to it.
• Know how to keep it up to date.
• Know what the school is doing to comply with its obligations under GDPR, the 1998 Act and the proposed 2018 Act.

The school/Trust will regularly provide all staff, parents, contacts and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the school holds and processes about them, and the reasons for which they are processed. This will be uploaded to the school websites.

All staff, parents and other users have a right under GDPR and the proposed 2018 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should contact the Designated Data Controller in writing on the form available.

The school/Trust does not make a charge if access is requested.

The school/Trust aims to comply with requests for access to personal information within one month in line with GDPR. The school and Trust email accounts are not monitored during the school holidays.

Subject Consent

Requests for information must be made in writing; which includes email, and be addressed to the Data Protection Officer. If the initial request does not clearly identify the information required, then further enquiries will be made. A subject access request form is on the school and Trust website.

The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of the relationship to the child. Evidence of identity can be established by requesting the production of two of the following:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive. The above document will be returned to the requested, once identity has been established.

Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand, and would not apply to Primary aged children, and the nature of the request.

GDPR and The proposed Data Protection Act 2018 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent will normally be obtained. There is still a need to adhere to the one month statutory timescale.

Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another will not be disclosed, nor will information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

If there are concerns over the disclosure of information, then additional advice will be sought.

Where redaction (information blacked out/removed) has taken place then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.

Information disclosed should be clear, thus any codes or technical terms will be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it will be retyped.

Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

The Trust has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for employment. The school/Trust has a duty of care to all staff and pupils and must therefore make sure that employees and those who use school facilities do not pose a threat or danger to other users.

The school may ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The school will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

The Trust will provide information to the police if they make a request to view data to prevent or detect crime or catch or prosecute a suspect.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the school is a safe place for everyone, or to operate other school policies, such as the leave of absence policy or the Equalities Statement. Because this information is considered special under GDPR and the proposed 2018 Act, staff (and pupils where appropriate) will be asked to give their express consent for the school to process this data.

Publication of School Information

Certain items of information relating to school staff will be made available via searchable directories on the public web site, in order to meet the legitimate needs of government agencies, researchers, visitors and enquirers seeking to make contact with the school. Staff may withdraw their consent for this information to be published, with the exception of the Head of School, SENCO and administrative contact.

Retention of Data

The school has a duty to retain some staff and student personal data for a period of time following their departure from the school, mainly for legal or safeguarding reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time, see data retention policy.

Conclusion

Compliance with GDPR and the proposed 2018 Act is the responsibility of all members of the Trust. All breaches must be reported immediately to the Head of School who will report to the DPO/DDPO. Breaches will be reported to the ICO within 72 hours. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.