THE HEATH ACADEMY TRUST

DATA PROTECTION POLICY

inspire transform together

Summary	
Policy Reference Number:	024
Category:	Data Protection
Authorised By:	Board Of Directors
Committee Responsible:	Board Of Directors
Version:	2019-1
Status:	21/03/2018: Approved at Full Trust Board. December 2018: Review of policy carried out by Trust DPO's (Jo Lolley & Selina White) 30/01/2019: Approved at Full Trust Board.
Next Review Date:	30/01/2020

The Heath Academy Trust
Registered Address: St. Ives Primary & Nursery School, Sandy Lane, St. Ives, Ringwood, Hampshire, BH24 2LE
Registered in England and Wales
Registration Number: 09809895

Contents

Definitions
Note: These terms are standard throughout all policy documents and are designed to provide clarity.

Section 1: The MAT

"the Academy Trust" *and* "Trust"	mean the Heath Academy Trust Company.
"the Board"	means the Board of Directors of the Heath Academy Trust Company.
"the Directors"	refers to the group of (up to 12) Directors who make up the Board, and who are also the Heath Academy Trust's "Trustees" under charity law.
"Finance Committee"	refers to the Finance and Audit Committee formed by the Board to manage the financial affairs of the Trust.
"Accounting Officer"	is a role held by the Chief Executive Officer ("CEO") of the Trust, and one which includes a personal responsibility for the financial resources under the Trust's control. He is accountable for the Trust's financial affairs.
"Chief Finance Officer" (CFO)	is the Trust's finance director, and also the Trust Business Manager, to whom the Accounting Officer delegates responsibility for delivery of the Trust's financial processes and reports , and for the oversight and consolidation of the Academies' financial data.
"Trust Business Manager" ("TBM")	Fulfils the CFO role within the Trust, including compliance and statutory returns, as described in the Academies' Financial Handbook.
"Leadership Team"	is a team representing the Academies, consisting of the Headteachers and the CEO, and the TBM.

A full description of the positions listed and their responsibilities will be found in the current Academies' Financial Handbook.

Section 2: The Schools

"Academy"	One of the six schools making up the Heath Academy Trust.
"Academies"	All of the six Academies.
"School"	means an Academy within the Trust.
"Finance Officer"	The person responsible for the day to day management of an Academy's financial operations.
"Governor"	means a formally elected and appointed member of a School's Governing Body (generally referred to as the LGB).
"Headteacher"	means the senior person at an Academy who may also be an Executive Headteacher and/or elected as a Director of the Board.
"School's Leadership Team"	A group within each School consisting of the Headteacher, senior staff and the local Governing Body.

1. Introduction

1.1 The Heath Academy Trust and its schools needs to gather and use certain information about individuals. These individuals can include pupils, parents/carers, employees, suppliers, business contacts and other people the schools and Trust have a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the Trust's data protection standards and to comply with the law.

1.2 This data protection policy ensures that The Heath Academy Trust:

- complies with data protection law and follows good practice
- protects the rights of pupils, staff, parents/carers and other stakeholders
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

1.3 This Data Protection policy is based on the eight principles of the Data Protection Act (DPA) that personal data shall be:

1. processed lawfully, fairly and in a transparent manner
2. collected for specified, explicit and legitimate purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. accurate and kept up to date
5. kept in a form which permits identification of data subjects for no longer than is necessary
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss or damage
7. processed in accordance with the rights of data subjects under this Act
8. restricted to use within the European Economic Area unless it can be guaranteed that there are adequate levels of protection of information.

2. Key Definitions

2.1 Data

2.1.1 The DPA describes how organisations, including The Heath Academy Trust must collect, handle and store personal information ('data').

2.1.2 Data is any information that the school and Trust collects and stores about individuals or organisations. Some data is more sensitive than others and particular care will be given to processing and managing this.

2.1.3 Sensitive data includes:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data; and
- biometric data.

2.1.4 Data can be stored electronically, on paper or on other materials.

2.1.5 To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

2.2 Data Subject

2.2.1 A 'Data Subject' is someone whose details the Trust and its schools keeps on file. The data subject has the following rights under data protection legislation:

- to be informed
- to have access to data stored about them (or their children)
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for the school to keep their data

- to restrict processing (e.g. limit what their data is used for)
- to object to data being shared or collected

2.2.2 Although data protection legislation affords these rights to individuals, in some cases the obligations schools and the Trust have to share data with the DfE etc. override these rights (this is documented later in the policy under 'Privacy Notices').

2.3 Data Protection Officers (DPO's)/Data Protection Controllers (DPC's)

2.3.1 The DPO's have overall responsibility for the personal data collected and processed and have a responsibility for ensuring compliance with the relevant legislation.

2.3.2 Each school within the Trust has a nominated DPO and DPC who will work in partnership with its' paired school to provide an independent overview of the work of that school's DPC.

3. Organisational Arrangements

3.1 Overall Responsibility

The Heath Academy Trust will meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective.

3.2 Roles & Responsibilities

3.2.1 The Trust Board will:

- Establish and maintain a positive data protection culture.
- Ensure the Data Protection Policy is approved and adopted by the Local Governing Body of each school and will review and monitor the effectiveness of the policy.
- Allocate sufficient resources for data protection, e.g. in respect of training for staff, encryption technology for devices.
- Monitor and review data protection issues.
- Ensure that the Trust provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities.
- Review and act upon data protection compliance reports from the Trust DPO's.

3.2.2 The Headteachers will:

- Nominate a DPC for their school and provide adequate resources and support for them to fulfil their statutory duties.
- Promote a positive data protection culture.
- Ensure that all staff co-operate with the Data Protection Policy.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to protect the data that they are processing.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.
- Monitor the work of the DPO's and DPC's to ensure they are fulfilling their responsibilities.

3.2.3 The DPO and DPC for each school will:

- Inform and advise the school of their obligations under data protection legislation.
- Monitor compliance with the legislation and report to the Headteacher/Local Governing Body and Trust Data Protection Officer on a termly basis. Clarify if this is being carried out.
- Cooperate with the supervisory authority e.g. Information Commissioners Office (ICO) and with the Trust DPO's act as the main contact point for any issues.
- Seek advice from other organisations or professionals, such as the ICO as and when necessary.
- Keep up to date with new developments in data protection issues for schools.
- Act upon information and advice on data protection and circulate to staff and governors.
- In conjunction with the Trust DPO's, carry out a data protection induction for all staff and keep records of that induction.

- Coordinate the school response to a Subject Access Request.
- Coordinate the school response to a data breach.

3.2.4 Staff at all Trust schools will:

- Familiarise themselves and comply with the Data Protection Policy.
- Comply with the Trust data protection arrangements.
- Follow the data breach reporting process.
- Attend data protection training as organised by the Trust.

4. Detailed Arrangements & Procedures

4.1 Data Management

4.1.1 Data Registration

As Data Controller, the Heath Academy Trust is registered with the ICO.

4.2 DPO's/DPC's

4.2.1 As a public body, The Heath Academy Trust is required to appoint a DPO and DPC).

4.2.2 At the Schools within the Trust the DPO/DPC role is fulfilled by:

• St. Ives Primary & Nursery School	Beverley Morris
• Three Legged Cross First & Nursery School	Stephanie Everett
• St. Mary's CE First & Nursery School	Kelly Davies
• Oakhurst Community First & Nursery School	Emma Hawkes
• St. James' CE First School	Sarah Riley
• Sixpenny Handley First School	Jayne Alford
• Trust Data Protection Officers	Jo Lolley/Selina White

4.2.3 The role of DPO for each school is outlined below

Jo Lolley
Three Legged Cross First & Nursery School
St. Mary's CE First & Nursery School
St. James' CE First School

Selina White
St. Ives Primary & Nursery School
Oakhurst Community First & Nursery School
Sixpenny Handley First School

4.2.4 The role of the DPO/DPC is to:

- Inform and advise the school and the employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws.
- Be the first point of contact for supervisory authorities.
- In conjunction with the Trust DPO's, coordinate training on data protection for all key stakeholders in the schools they are responsible for.

4.3 Data Protection Awareness

4.3.1 In order to ensure organisational compliance, all staff and other key stakeholders (e.g. governors, volunteers) will be made aware of their responsibilities under the data protection legislation as part of their induction programme, (both as a new employee/governor to the organisation or if an individual changes role within the school).

4.3.2 The Trust DPO's will ensure annual data protection refresher training will take place to reinforce the importance of staff adhering to the legislation.

4.3.3 A record of the professional development undertaken by the individual will be retained on their training record.

5. Data Mapping

5.1 Each School and the Trust central team has documented all of the data that it collects within a 'Data Flow Map'. This data inventory records:

- the data held
- what the data is used for
- how it is collected
- how consent is obtained
- how the data is stored
- what the retention period is
- who can access the data
- who is accountable for the data
- how the data is shared
- how the data is destroyed

5.2 For each data type, the probability of a data breach occurring is assessed (very high, high, medium, low or very low) and actions to be taken to mitigate the risk are recorded.

5.3 It is the responsibility of the DPO/DPC to ensure the 'Data Flow Map' for the Trust (DPO) and school (DPC) is kept up to date. The map should be a live document and updated regularly.

6. 3rd Party Suppliers Acting As Data Processors

6.1 As Data Controller, the school is responsible for ensuring that correct protocols and agreements are in place to ensure that personal data is processed by all sub-contractors and other third parties in line with the principles of the data protection legislation.

6.2 Individuals within school who have a responsibility for securing contracts and agreements with such third parties are responsible for ensuring that all external data processing is contracted out in line with the principles of the DPA. These type of agreements include:-

- data and hard copy documents.
- Data destruction and hardware renewal and recycling financial and personnel information.
- Pupil and staff records.

6.3 Only 3rd party suppliers who can confirm they have appropriate technical, physical and organisational security to securely process data will be considered as suitable partners.

6.4 The procurement process will ensure that all contracts are suitable and reflect DPA requirements. Review of current and due consideration of future contracts will require this even if data processing is ancillary to the main purpose of the contract.

6.5 The external processor will confirm with the DPO/DPC that suitable security and operational measures are in place.

6.6 Any potential supplier or purchaser outside the EU will be obliged to confirm how they comply with the DPA and give contractual assurances.

6.7 The DPO/DPC may require a specific risk assessment to be undertaken if the data is sensitive, and if an increased risk is likely due to the nature, or proposed nature, of the processing.

6.8 A written agreement will be in place between the supplier and the school to confirm compliance with the DPA principles and obligations to assist the school in the event of data breach or subject access request, or enquiries from the ICO.

6.9 The school must have the right conduct audits or have information about audits that have taken place in respect of the relevant processes of the supplier's security arrangements whilst the contract is in place, or whilst the supplier continues to have personal data that relates to the contract on its systems.

6.10 Any subcontracting must only be done with the written consent of the school as data controller. This must be the case for any further subcontracting down the chain. All subcontractors must confirm agreement to be bound by DPA principles when handling the school's data, which shall also include co-operation and eventual secure destruction or return of data.

6.11 The school has a '3rd Party Request for Information Process' which must be used for 3rd party suppliers acting as a Data Processor for the school.

7. Consent

7.1 As a Trust we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases, data will only be processed if explicit consent has been obtained.

7.2 Consent is defined by the DPA as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

7.3 We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

8. Privacy Notices

8.1 In order to comply with the fair processing requirements of the DPA, the school will inform their staff and parents/carers of all pupils of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom their data may be passed, through the use of 'Privacy Notices'.

8.2 Privacy notices are available to staff and parents through the following means:

- School website
- School newsletter
- School prospectus
- Letter to parents
- Staff Handbook
- Staff notice boards

9. The Use Of Pupil Images

9.1 Occasionally the school may take photographs of its pupils. These images could be used as part of internal displays, printed publications, the school website or our social media accounts.

9.2 The school will seek consent from all parents to allow the photography of pupils and the subsequent reproduction of these images. Consent will be sought on an annual basis.

9.3 Parents are given the opportunity to opt in. It is not permissible to assume parents are opting in. Generic consent for all uses of images is not acceptable; parents must give consent to each medium.

9.4 Parents must be given the opportunity to withdraw their consent at any time. This should be given in writing to the school, however a verbal withdrawal of consent is also valid and should be reported to the DPO/DPC immediately.

9.5 Consent should be recorded *school to insert process for recording parental consent, e.g. logged on Sims.*

9.6 If images of individual pupils are published, then the name of that child should not be used in the accompanying text or caption unless specific consent has been obtained from the parent prior to publication.

9.7 The School 'Parental Consent' form should be issued to current parents to seek consent annually.

10. Accurate Data

10.1 The school will endeavour to ensure that the data it stores is accurate and up to date.

10.2 When a pupil or member of staff joins the school/Trust they will be asked to complete a form providing their personal contact information (e.g. name, address, phone number, NI number for staff)next of kin details, emergency contact and other essential information). At this point, the school/Trust will also seek consent to use the information provided for other internal purposes (such as promoting school events, photography).

10.3 The school will undertake an annual data collection exercise, where current staff and parents will be asked to check the data that is held about them is correct. This exercise will also provide individuals with the opportunity to review the consent they have given for the school/Trust to use the information held for internal purposes.

10.4 Parents/carers and staff are requested to inform the school/Trust when their personal information changes.

11. Withdrawal Of Consent

11.1 Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the school will consider each situation on the merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

11.2 Parents/carers and staff are requested to complete a 'Withdrawal Of Consent' form and return this to the DPO/DPC.

12. Associated Data Protection Policies

- Complaints
- Data Breach Procedure
- Record Management & Retention
- Subject Access Request
- 3rd Party Requests For Information Process
- Bring Your Own Device Policy
- Disciplinary and Capability Policy

13. Complaints

13.1 Complaints will be dealt with in accordance with the Trust Complaints Policy.

14. Data Breaches

14.1 Although the Heath Academy Trust takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space).
- Unforeseen circumstances such as fire or flood.
- Hacking attack.
- 'Blagging' offences where information is obtained by deceiving the Heath Academy Trust and its schools.
- The school has a Data Breach Procedure which sets out the process that should be followed in the event of a data breach occurring.

15. Privacy Impact Assessments

15.1 When considering the purchase of a new service or product that involves processing personal data, a Data Privacy Impact Assessment must be completed by the DPO/DPC. If risks are identified as part of the assessment then appropriate steps to mitigate this risk must be implemented. If these risks are deemed to be 'high risk' then the DPO/DPC should consult with the ICO prior to implementation.

15.2 The 'Data Privacy Impact Assessment Form' must be used for each new service/product.

16. Records Management

16.1 The Heath Academy Trust recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations which will also contribute to the effective overall management of the school.

16.2 The Trust has a Data Record Management & Retention Policy in place which sets out how it will:

- safely and securely store data (both digital and hard copy data)
- retain data
- dispose of data

17. Subject Access Requests

17.1 Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the school/Trust holds about them and can make a Subject Access Request (SAR).

17.2 The Trust has a SAR Policy, which sets out the process that should be followed in the event of receiving a SAR.

18. 3rd Party Requests For Information

18.1 Occasionally the Trust may receive a request for information on a pupil or member of staff by a third party, such as the police or social services. This would be separate to statutory requests that come through from the DfE or LA, for example, which are covered within the privacy notices.

18.2 The Trust has a 3rd Party Request For Information Process which sets out the process that should be followed in the event of receiving a 3rd party request.

19. Use Of Personal Devices

19.1 The Heath Academy Trust recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices. All staff, governors, trustees, contractors and visitors are expected to follow the Bring Your Own Device Policy which sets out how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school.