OVERARCHING DATA PROTECTION POLICY

Document Details	
Policy author	Chief Finance and Operations Officer
Authorised By	Trust Board
Date of Approval	December 10th 2025
Date for Review	Annual

V 25.2

Changes October 2025

3.3	Updated Complaints section to align with ICO expectations Annual consent from Southview school removed. Lifetime consent for all schools added.
Throughout	Director of Operations replaced with Chief Finance and Operations Officer

Changes Feb 2025

3.4	AI usage statement included under Data Breach
Throughout	“governors” replaced with Local advisory committees (LAC)

Changes to previous edition May 2024

2.2	Director of Operations added as policy author.
3.1	New registration date inserted
3.4	ICT Usage agreements – inclusion of parents and pupils

CONTENTS

1. Introduction & Key Definitions....4

1.1. Introduction....4

1.2. Key Definitions....4

2. Organisational Arrangements....5

2.1. Overall responsibility....5

2.2. Roles and Responsibilities....5

3. Detailed Arrangements and Procedures....7

3.1. Data Management....8

- Data Registration
- Data Protection Officer
- Data Protection Awareness
- Data Mapping

3.2. Third Party Suppliers Acting as Data Processors....8

3.3. Consent....9

- Privacy Notices
- The Use of Pupil Images
- Accurate Data
- Withdrawal of Consent
- Complaints

3.4. Associated Data Protection Policies....10

- CCTV
- Confidentiality Agreement
- Data Breaches
- Artificial Intelligence (AI)
- Data Privacy Impact Assessments
- ICT Usage Agreement
- Records Management & Retention
- Subject Access Requests
- Third Party Requests for Information

Hope Learning Community is a Charitable company Limited by Guarantee. Company Number: 10391530, Registered in England & Wales.
Registered Office: Market Field School, School Road, Elmstead Market, Colchester, CO7 7ET

Part 1 Introduction and Key Definitions

1.1 Introduction

Hope Learning Community and its schools and college, needs to gather and use certain information about individuals.

These individuals can include pupils, parents/carers, employees, suppliers, business contacts and other people the trust has 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.

This data protection policy ensures Hope Learning Community and its schools and college:

- 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

This data protection policy is based on the six principles of the Data Protection Act (DPA) 2018 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

1.2 Key Definitions

Data

The DPA describes how organisations, including Hope Learning Community, must collect, handle and store personal information ('data').

Data is any information that the 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. 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.

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

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

Data Subject

A 'Data Subject' is someone whose details the trust 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 in 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

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

Data Controller

The 'Data Controller' has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf.

The Hope Learning Community is the 'Data Controller'.

Data Processor

A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorised to collect or has already collected. It can be a member of staff or a third party company such as a curriculum software provider or a payroll provider.

Part 2 Organisational Arrangements

2.1 Overall Responsibility

Hope Learning Community 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.

2.2 Roles & Responsibilities

The Trust Board will:

- Establish and maintain a positive data protection culture.
- Ensure the Director of Operations prepares a Data Protection policy for approval and adoption by the Trust Board and to review and monitor the effectiveness of the policy.
- Appoint a Data Protection Officer and provide adequate resources and support for them to fulfil their statutory duties.

- 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 Data Protection Officer.
- Attend data protection training as organised by the trust.

The CEO will:

- Promote a positive data protection culture.
- Ensure that all headteachers/head of schools co-operate with the policy.
- Ensure that trustee and Headteacher/Head of School induction includes information on data protection and keep records of that induction.
- Ensure that trustees are provided with annual data protection training and that records of this are maintained
- Monitor the work of the Data Protection Officer to ensure they are fulfilling their responsibilities.

The Data Protection Officer will:

- Inform and advise the Hope Learning Community of their obligations under data protection legislation.
- Monitor compliance with the legislation and report to the CEO and Trust Board on a termly basis.
- Co-operate with the supervisory authority (e.g. Information Commissioner's Office) and act as the main contact point for any issues.
- Seek advice from other organisations or professionals, such as the Information Commissioner's Office as and when necessary.
- Keep up to date with new developments in data protection issues for schools.
- Advise and guide the Hope Learning Community on subject access requests and data breaches.

The Chief Finance and Operations Officer will:

- Prepare a Data Protection Policy for approval by the Trust Board, revise as necessary and review annually

The Director of Governance and Compliance will:

- Act upon information and advice on data protection and circulate to staff, trustees and Local Advisory Committee members (LACs)
- Coordinate data protection training for trustees and LACs
- Coordinate the response to a Subject Access Request.
- Coordinate the response to a data breach.

.

The Headteacher/Head of school and Local Advisory Committees will:

- Ensure that all staff co-operate with the 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.

The Local Data Protection Lead will:

- Ensure that staff and LAC induction includes information on data protection and keep records of that induction.
- Ensure that staff and LAC members are provided with annual data protection training and that records are maintained.
- Ensure the 'Data Flow Map' is kept up to date.

All Staff at the school will:

- Familiarise themselves and comply with the Data Protection Policy.
- Comply with the Hope Learning Community data protection arrangements.
- Follow the data breach reporting process.
- Attend data protection training as organised by the school/college.

Part 3 Detailed Arrangements & Procedures

3.1 Data Management

Data Registration

As Data Controller, the Hope Learning Community must register as a Data Controller on the Data Protection Register held by the Information Commissioner. The trust was last registered on 04/11/2024 and is due for renewal on 03/11/2025.

Data Protection Officer

As a public body, Hope Learning Community is required to appoint a Data Protection Officer (DPO).

At Hope Learning Community the DPO role is fulfilled by:

- SBM Services (UK) Ltd

The link between the school and SBM Services (UK) Ltd is the Director of Governance and Compliance, who will be the key point of contact.

The role of the DPO is to:

- Inform and advise the school/academy 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.

Data Protection Awareness

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

Staff and trustees/LAC members will also be required to complete annual cyber security training to ensure that they are aware of cyber risks and understand the important role that they play in reducing the risk of a successful cyber-attack.

Annual data protection refresher training will take place to reinforce the importance of staff, Local Academy Committee memberss and trustees adhering to the legislation.

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

Data Mapping

Hope Learning Community and its schools and college has documented all of the data that it collects within 'Data Flow Maps'. 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

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.

It is the responsibility of the Data Protection Lead in each school/college to ensure the 'Data Flow Map' is kept up to date. The map should be a live document and updated regularly.

3.2. Third Party Suppliers Acting as Data Processors

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

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:-

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

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

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.

The external processor will confirm with the data controller that suitable security and operational measures are in place.

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

The DPO 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.

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

The trust must have the right to 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.

Any subcontracting must only be done with the written consent of the trust 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 trust's data, which shall also include cooperation and eventual secure destruction or return of data.

The trust has a 'Third Party Request for Information' form which must be used for third-party suppliers acting as a Data Processor for the trust.

The trust maintains evidence of the checks that have taken place for each of their third-party suppliers.

3.3. Consent

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.

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".

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

As Hope Learning Community has secondary settings, we will seek direct consent from pupils for:

- use of images
- releasing information related to subject access requests.

When they reach age 13 and have the competence to understand the consequences of consenting and can give informed consent.

Privacy Notices

In order to comply with the fair processing requirements of the DPA, the trust will inform their staff, parents/carers of all pupils and Local Academy Committee memberss/trustees 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'.

Privacy notices are available to staff, parents and trustees/LAC members through the following means:

- School website
- School newsletter

- School prospectus
- Letter to parents
- Staff Handbook
- Staff Notice Boards

Privacy notices will be reviewed on an annual basis.

The Use of Images (Pupil & Staff)

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

Hope Learning Community will seek consent from all parents to allow the photography of pupils and the subsequent reproduction of these images. Consent will be sought from pupils age 13 and over for the use of images and prior to releasing information related to a subject access request where they have the competence to understand the consequences of consenting and can give informed consent

Consent will last for the length of time the child is a pupil at the school/college.

Hope Learning Community will seek consent from all members of staff to allow their photography and the subsequent reproduction of these images.

Parents and staff are given the opportunity to opt in. It is not permissible to assume they are opting in.

Generic consent for all uses of images is not acceptable; parents and staff must give consent to each medium.

Parents and staff 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 school office immediately.

Consent should be recorded on the school/college management information system.

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.

The trust's 'Parental Consent' and 'Staff Consent' forms are used to seek consent when they join the organisation.

Accurate Data

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

When a pupil or member of staff joins the 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 trust will also seek consent to use the information provided for other internal purposes (such as promoting school events, photography).

The trust 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 trust to use the information held for internal purposes.

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

Withdrawal of Consent

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 trust will consider each situation on its merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

Parents/carers and staff are requested to complete a Withdrawal of Consent form and return this to the relevant school/college office.

Complaints

If an individual believes the trust has mishandled their personal data or that their data protection rights have been breached, they have the right to make a complaint.

Concerns or complaints should be directed as follows:

Director of Governance and Compliance

governance@hopelearningcommunity.org.uk

Complaints will be acknowledged by the trust at the earliest opportunity, but at the latest within 30 days.

The trust will take reasonable steps to investigate the concern without undue delay.

The individual that has raised the complaint will be informed of the outcome once the investigation has concluded.

If the individual is unsatisfied with how the complaint has been managed, they can escalate their concern to the Information Commissioner.

Website: Make a complaint about how an organisation has used your personal information | ICO

Phone: 0303 123 1113

3.4. Associated Data Protection Policies

- CCTV
- Complaints
- Confidentiality Agreement
- Cyber Security
- Data Breaches
- Data Privacy Impact Assessments
- ICT Usage Agreement
- Records Management & Retention
- Subject Access Requests
- Third Party Requests for Information
- Use of Personal Devices

CCTV

Hope Learning Community uses closed circuit television (CCTV) images to reduce crime and monitor the buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the school property. Each school has a CCTV Policy in place which documents:

- why CCTV is used
- where cameras are sited
- whether covert monitoring is undertaken
- how long images are retained for
- who has access to the images
- what the complaints procedure is

Confidentiality Agreement

The trust has a Confidentiality Agreement in place which staff, Local Academy Committee members/trustees and volunteers are required to sign on an annual basis. This agreement sets out the expectations the trust has in relation to maintaining confidentiality.

Cyber Security

The trust has created a policy to help outline the security measures put in place and the expectations of people with access to its systems to ensure information remains secure and protected and the risk of cyber-attacks reduced.

Data Breaches

Although the 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 trust.

The trust has a Data Breach policy which sets out the process that should be followed in the event of a data breach occurring.

AI (Artificial Intelligence)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Hope Learning Community recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Hope Learning Community will treat this as a data breach, and will follow the personal data breach procedure outlined in our Data Breach Policy.

Data Privacy Impact Assessments

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 school/college in conjunction with their Data Protection Lead. 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 should consult with the ICO prior to implementation.

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

ICT Usage Agreements

The trust has an ICT Usage Agreement in place which staff, Local Academy Committee members/trustees, volunteers, parents and pupils are required to sign on an annual basis. This agreement sets out the expectations the trust has in relation to staff safely and securely using the IT network.

Records Management

The 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.

The trust has a 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
- protect IT Hardware, software and access to online systems

The retention schedule is based on the good practice advice provided by the Institute of Records Management Society (IRMS) for schools.

Subject Access Requests

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

The trust has a Subject Access Request Policy, which sets out how a SAR can be made and the process that should be followed in the event of receiving a SAR.

Third Party Requests for Information

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.

The trust has a Third Party Request for Information Policy which sets out the process that should be followed in the event of receiving a third party request.

Use of Personal Devices

The trust recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices. The trust follows the 'Bring Your Own Device' Policy which sets out the limits to permitted use of non-school owned electronic devices, e.g. laptops, smartphones and tablets by staff members and visitors to the school.