

Liberty Academy Trust

Data Protection Policy

Date	September 2026
Written By	Director of Governance and Compliance
Approve by Executive	September 2026
Review Date	September 2028

Table of Contents

1	Policy statement	3
2	About this policy.....	3
3	Definition of data protection terms	3
4	Data protection officer	3
5	Responsibilities.....	4
6	Our data protection commitments	4
7	Data protection principles	5
8	Legal grounds for processing	6
9	Data subjects' rights.....	8
10	Subject Access Requests	9
11	Right of Access	11
12	Automated decision-making and profiling.....	13
13	Data security	14
14	Personal data breaches.....	15
15	Disclosure and sharing of personal information	16
16	Data processors.....	16
17	Images and videos.....	16
18	Video Surveillance.....	17
19	Biometric Data.....	17
20	Complaints	18
21	Disposal of data.....	18
22	Training	18
23	Complaints	18
24	Changes to this policy	19
25	Social responsibility statement:	19
	Appendix 1.....	20
	Appendix 2	22

Key Information

Data protection officer (DPO): Christopher Rossiter

Contact details: dpo@libertytrust.org.uk

References to external sources:

- [Department for Education's Data Protection in Schools toolkit.](#)
- [ICO's FOIA publication scheme for schools in England](#)

1 Policy statement

- 1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as an academy trust ("Trust"), we will collect, store and process personal data about our pupils, staff, parents and others. This makes us a data controller in relation to that personal data.
- 1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.
- 1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data**. This policy sets out how we comply with the relevant legislation. Breaches of this policy can result in the risk of real harm to individuals, action for damages, loss of trust and reputational harm as well as regulatory penalties, including fines.
- 1.4 All **data users** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action. Individuals may be prosecuted for committing offences under sections 170-173 of the Data Protection Act 2018.

2 About this policy

- 2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the retained EU law version of the General Data Protection Regulation ((EU)2016/679) ('UK **GDPR**'), the Data Protection Act 2018 and other regulations (together '**data protection legislation**').
- 2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.
- 2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.
- 2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3 Definition of data protection terms

- 3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

4 Data protection officer

- 4.1 As a Trust, we are required to appoint a data protection officer ("**DPO**"). Our DPO is Christopher Rossiter, and they can be contacted at dpo@libertytrust.org.uk.
- 4.2 The DPO is responsible for informing and advising the Trust about **data protection legislation**, ensuring compliance with the **data protection legislation** and with this policy. Any questions about the operation of this policy, or any concerns that the policy has not been followed should be referred in the first instance to the DPO.
- 4.3 The DPO is also the central point of contact for all **data subjects, the Information Commissioner's Office ("ICO")** and others in relation to matters of data protection.

5 Responsibilities

This policy applies to all staff, contractors, Trustees, Local Committee Members and volunteers.

5.1 Principals

The school Principal is responsible for ensuring that effective data management practices are maintained in school on a day-to-day basis in our schools.

5.2 IT and data team

LAT's IT team (including staff and contractors) are responsible for ensuring all data systems are secure in line with the requirements set out by the ICO and the DfE's digital standards.

The Director of Digital Innovation is responsible for maintaining the Trust's register of processing activity, reviewing and preparing DPIAs.

5.3 All staff

LAT staff are responsible for:

- Adhering to this policy whilst using, collecting, storing and processing data.
- Reporting concerns that relate to the use, collection and storage of data and, the possible damage or loss of that data to the DPO.
- Maintaining their own personal data held on staff records.

6 Our data protection commitments

- 6.1 We are dedicated to ensuring that **personal data** is processed in alignment with the legal principles of data protection.

- 6.2 We implement a strategy focused on “Data Protection by Design and Default”.
- 6.3 We can prove our adherence to **data protection legislation**.
- 6.4 **Data subjects** are well informed about how and why we use their data, and they can exercise their rights regarding their data.
- 6.5 We share **personal data** only when it is fair and lawful, ensuring that any data sharing is conducted securely.
- 6.6 We handle and report all **personal data breaches**, including minor ones, effectively to mitigate any potential risks and to improve our practices.

7 Data protection principles

- 7.1 Anyone **processing personal data** must comply with the data protection principles. We will comply with these principles in relation to any **processing of personal data** by the Trust.
- 7.2 The principles provide that **personal data** must be:
- **Processed** fairly, lawfully, and transparently in relation to the **data subject**. This means that we only use **personal data** with respect for the individual who it relates to, in line with the legal grounds for **processing**, and we inform **data subjects on** how their **personal data** is **processed** including, among other ways, in our **privacy notices**.
 - **Processed** for specified, explicit, and legitimate purposes, and in a way which is not incompatible with those purposes. This means that if we collect **personal data** for one purpose and then need to use it for another reason, we will ensure that new purpose is compatible with the original reason for **processing**.
 - Adequate, relevant, and not excessive for the purpose. This means that we will collect enough information to achieve our aim, whilst minimising that collection to what is genuinely required.
 - Accurate and up to date. This means that we will try to ensure that **personal data** is accurate when we collect it and kept up to date over time.
 - Not kept for any longer than is necessary for the purpose. This means that we will only keep **personal data** for as long as is necessary in accordance with our [Data Retention Policy]; and
 - **Processed** securely using appropriate technical and organisational measures. Our measures include; technical safeguards like security of ICT systems, control over ICT access, the use of pseudonyms and encryption, as well as organisational safeguards, including plans for business continuity, securing our premises and data physically, implementing policies and procedures, conducting regular training, and carrying out audits and evaluations of operational measures and strategic oversight of compliance.

7.3 **Personal data** must also:

- Be **processed** in line with **data subjects'** rights.
- Not be transferred to people or organisations situated in other countries without adequate protection.

8 **Legal grounds for processing**

8.1 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the **data protection legislation**. We will normally **process personal data** under the following legal grounds:

- Where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract.
- Where the **processing** is necessary to comply with a legal obligation that we are subject to.
- Where the **processing** is necessary in order to protect the vital interests of a **data subject** or another individual.
- Where the law otherwise allows us to **process** the **personal data**, or we are carrying out a task in the public interest.
- Where the **processing** is necessary for the purposes of a recognised legitimate interest as set out in Annex 1 of the **GDPR**.
- Where we are pursuing legitimate interests, (or the legitimate interests of a third party), except where such interests are overridden by the interests or fundamental rights and freedoms of **data subjects**; and
- Where none of the above apply, then we will seek the consent of the **data subject** to the **processing** of their **personal data**.

8.2 When **special category personal data** is being processed, then an additional legal ground must apply to that processing. We understand that for certain types of **processing** of **special category personal data**, we must have, and comply with, an appropriate policy document. Our special category personal data policy is our appropriate policy document for these purposes.

8.3 We will normally only **process special category personal data** under following legal grounds:

- Where the **processing** is necessary for employment law purposes, for example, in relation to sickness absence.
- Where the **processing** is necessary for reasons of substantial public interest, for example, for the purposes of equality of opportunity and treatment.
- Where the **processing** is necessary for health or social care purposes, for example, in relation to pupils with medical conditions or disabilities; and
- Where none of the above apply, then we will seek the explicit consent of the **data subject** to the **processing** of their **special category personal data**.

- 8.4 We will inform **data subjects** of the above matters by way of appropriate **privacy notices**, which shall be provided to them when we collect the data, or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.
- 8.5 If any **data user** is in doubt as to the legal ground for processing **personal data** for any purpose, then they must contact the DPO before doing so.

Vital Interests

- 8.6 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not able to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances, we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

- 8.7 Where none of the other bases for **processing** set out above apply, then the Trust must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.
- 8.8 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.
- 8.9 When pupils and/or our **workforce** join the Trust, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate, third parties may also be required to complete a consent form.
- 8.10 In relation to all pupils under the age of 13 years old we will seek consent from an individual with parental responsibility for that pupil.
- 8.11 We will generally seek consent directly from a pupil who has reached the age of 13, however we recognise that this may not be appropriate in certain circumstances or in relation to personal capacity, and therefore we may be required to seek consent from an individual with parental responsibility.
- 8.12 If consent is required for any other **processing** of **personal data** of any **data subject**, then the form of this consent must:
- Inform the **data subject** of exactly what we intend to do with their **personal data**.
 - Require them to positively confirm that they consent – we cannot ask them to opt out rather than opt in; and

- Inform the **data subject** of how they can withdraw their consent.

- 8.13 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent. We will ensure that it will be as easy for the **data subject** to withdraw their consent as it was to give it.
- 8.14 Consent may need to be refreshed where we need to process the **personal data** for a different and incompatible purpose, which was not disclosed when the consent was first considered by the **data subject**.
- 8.15 The DPO must always be consulted in relation to any consent form before consent is obtained.
- 8.16 A record must always be kept of any consent, including how it was obtained and when.

9 Data subjects' rights

- 9.1 In addition to the right to be informed and the right to withdraw consent, we will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:
- Request access to any **personal data** we hold about them.
 - Object to the **processing** of their **personal data**, including the right to object to direct marketing.
 - Have inaccurate or incomplete **personal data** about them rectified.
 - Restrict **processing** of their **personal data**.
 - Have **personal data** we hold about them erased.
 - Have their **personal data** transferred; and
 - Object to the making of decisions about them by automated means.
- 9.2 The rights available to **data subjects** will depend on the lawful basis for **processing**, for example, where **personal data** is **processed** under the lawful basis of public task, then the **data subject** cannot withdraw consent for such **processing**, but they can exercise the right of objection.
- 9.3 Except for the right to object to direct marketing, other rights requests in an education or employment context can be complex. We will comply with our obligations under **data protection legislation** and the guidance given by the **ICO** in respect of individuals seeking to exercise their rights.
- 9.4 We will consider **data subject** requests and provide a response within one month, except if we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the **data subject** within one month of their request that this is the case.
- 9.5 Where we are unable to grant **data subjects** any requests made as part of

their rights, for example, where we are unable to delete data as we are required to retain it in relation to any claim or legal proceedings, we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Trust and to the **ICO** at the time that we inform them of our decision in relation to their request.

9.6 The DPO must be consulted in relation to any data subject rights request.

The right of access to personal data

9.7 **Data subjects** may request access to the **personal data** we hold about them and which we are able to provide based on a reasonable and proportionate search for that **personal data**. Such requests will be considered in line with the Trust's subject access request procedure.

Data protection by design and default

9.8 The Trust will consider and comply with the requirements of **data protection legislation** in relation to all of its activities whenever these involve the use of **personal data**, in accordance with the principles of data protection by design and default.

9.9 In certain circumstances, where the law requires us to, we shall carry out detailed assessments of proposed processing in a **data protection impact assessment** ("DPIA"). This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing**, or there is a change in our existing ways of working.

9.10 The Trust will complete a **DPIA** of any such proposed **processing**, and has a template document, which ensures that all relevant matters are considered. We may also carry out **DPIAs** where one is not legally required, as a matter of good practice.

9.11 The DPO should always be consulted as to whether a **DPIA** is required, and if so, how to undertake that assessment. The DPO must always be consulted where **personal data** is to be transferred to different countries to ensure adequate protection is in place.

10 Subject Access Requests

10.1 Right of Access

Individuals have the right to request access to the personal data that the Trust holds about them. This is known as a Subject Access Request (SAR).

A SAR can be made verbally or in writing and may be submitted to any member of staff. All SARs must be logged on the SchoolPro platform and shared immediately with the DPO.

When responding to a SAR, the Trust will:

- verify the identity of the requester where necessary;
- provide a copy of the personal data requested and any supplementary information required by data protection law;
- respond without undue delay and normally within one month of receiving the request;
- provide information free of charge, unless the request is manifestly unfounded or excessive; and
- provide the information electronically where the request is made electronically, unless another format is requested.

Where a request is complex or numerous, the Trust may extend the response period by up to a further two months. The requester will be informed of any extension and the reasons for it within one month of receipt of the request.

The Trust may refuse a request or charge a reasonable fee where permitted by data protection legislation. Where a request is refused, the Trust will explain the reasons and inform the individual of their right to complain to the Information Commissioner's Office (ICO) or seek a remedy through the courts.

10.2 Children and Subject Access Requests

Personal data belongs to the individual to whom it relates. A child may make a SAR on their own behalf where they are considered capable of understanding their rights and the implications of the request.

A parent or person with parental responsibility may make a SAR on behalf of a child where the child lacks the necessary understanding or has authorised the request.

The Trust will assess a child's capacity to exercise their data protection rights on a case-by-case basis and will not make decisions solely on the basis of age or any special educational need or disability.

Parents may also have a right to access their child's educational record under separate education legislation. Requests for educational records will be dealt with in accordance with Section 15 of this policy.

10.3 Limitations on Disclosure

The Trust may withhold information where disclosure is exempt under data protection legislation, including where disclosure would:

- adversely affect the rights and freedoms of another individual;

- cause serious harm to the physical or mental health of any person;
- prejudice the prevention or detection of crime or the apprehension or prosecution of offenders; or
- otherwise fall within an applicable statutory exemption.

11 Right of Access

Any person may request information held by the Trust under the Freedom of Information Act 2000 (FOIA).

Requests must be made in writing (including by email), state the applicant's name and correspondence address, and describe the information requested clearly enough for it to be identified. Requests for environmental information may be made verbally under the Environmental Information Regulations 2004 (EIR), although written requests are preferred.

The Trust will normally respond within 20 school days or 60 working days, whichever is shorter.

When responding, the Trust will:

- confirm whether the requested information is held;
- provide the information unless an exemption applies;
- explain any refusal or partial refusal;
- provide details of the internal review process; and
- explain the right to complain to the Information Commissioner's Office (ICO).

The Trust may refuse a request where:

- further clarification has been requested but not provided;
- the information is exempt from disclosure;
- the cost of compliance exceeds the statutory limit;
- the request is vexatious or repeated; or
- any applicable fee has not been paid.

11.1 Exemptions

Where information is held, the Trust will consider whether it can be disclosed or whether an exemption applies under FOIA. Common exemptions include:

- **Section 21** – information already reasonably accessible to the requester.
- **Section 22** – information intended for future publication.
- **Section 31** – disclosure would prejudice the prevention or detection of crime.
- **Section 36** – disclosure would prejudice the effective conduct of public affairs.

- **Section 38** – disclosure would endanger an individual's physical or mental health or safety.
- **Section 40(1)** – the request relates to the requester's own personal data and should be dealt with as a Subject Access Request.
- **Section 40(2)** – disclosure would involve the personal data of a third party and would breach data protection legislation.
- **Section 41** – information provided in confidence.

Some exemptions are **qualified exemptions**, meaning the Trust must consider whether the public interest in disclosure outweighs the exemption before deciding whether to withhold the information.

11.2 **The Appropriate Limit**

The Trust is not required to comply with a request where the estimated cost of determining, locating, retrieving and extracting the information exceeds the statutory limit, currently £450 (equivalent to 18 staff hours).

When making this estimate, the Trust may only take account of the activities permitted under the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

Where appropriate, the Trust will provide advice and assistance to help the requester refine the request.

11.3 **Charging Fees**

The Trust may charge fees permitted under FOIA, including reasonable costs for printing, photocopying and postage.

Where a fee applies, a fees notice will be issued and the Trust will not be required to provide the information until payment has been received.

11.4 **Providing Advice and Assistance**

The Trust will provide reasonable advice and assistance to help applicants make effective requests, including:

- seeking clarification where necessary;
- helping applicants refine requests that exceed the cost limit; and
- directing applicants to information that is already publicly available.

The Trust is not required to provide advice and assistance in relation to vexatious or repeated requests.

11.5 **Vexatious Requests**

The Trust is not required to comply with vexatious requests.

Whether a request is vexatious will be considered on a case-by-case basis, taking account of:

- the burden placed on the Trust;
- the purpose and value of the request;
- the conduct and motive of the requester; and
- any harassment, distress or disruption caused to staff.

Where a request is refused as vexatious, the applicant will be informed of the decision and their rights to request an internal review and complain to the ICO.

11.6 Internal Review

Applicants may request an internal review if they are dissatisfied with the Trust's response.

Requests for review should normally be submitted within two months of the response. Reviews will be conducted by an individual not involved in the original decision, wherever possible.

The Trust will aim to communicate the outcome of the review within 20 working or school days, depending on the nature of the request.

Following an internal review, applicants may complain to the ICO if they remain dissatisfied.

12 Automated decision-making and profiling

12.1 The Trust does not routinely make decisions about individuals solely by automated means. Examples of automated **processing** that may be used within an educational setting include:

- Recruitment systems filtering or scoring applications.
- Behaviour or safeguarding systems identifying patterns or risks.
- Assessment platforms that automatically mark or analyse pupil performance.

12.2 Where automated **processing** produces outcomes that inform or influence decisions, the Trust will seek to ensure that meaningful human involvement (using so-called 'human in the loop' processes) such as review, oversight, or the ability to amend outcomes, is applied as part of the decision-making process.

12.3 Where a decision is made solely by automated means and produces legal or similarly significant effects on a **data subject**, the **data subject** has the right to:

- Be informed that such a decision has been made.
- Make representations about the decision.
- Request that a human review the decision; and
- Contest the outcome of the decision.

- 12.4 The Trust will ensure that appropriate processes are in place to receive and respond to such requests in a timely manner.
- 12.5 Where automated decision-making involves the **processing** of **special category personal data**, such **processing** will only take place where:
- The individual has given explicit consent; or
 - The **processing** is necessary for reasons of substantial public interest and is either: (i) necessary for entering into, or performing, a contract between the individual and a **controller**; or (ii) required or authorised by law.
- 12.6 The Trust will keep its approach to automated decision-making under review and will seek further advice where necessary, particularly in relation to new technologies or AI-based systems. Where the Trust's **processing** activities are also subject to EU GDPR, individuals may hold broader rights in this area, and the Trust's **privacy notices** will reflect the applicable legal framework accordingly.

13 Data security

- 13.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.
- 13.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.
- 13.3 Security procedures include:
- **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the DPO within 24 hours.
 - **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (**Personal data** is always considered confidential.)
 - **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the **ICO** guidance on the disposal of IT assets.
 - **Paper records.** Data users must minimise the storage and use of paper records. All internal documents, including forms, should be held digitally. All paper records relating to pupils should be digitalised and disposed of within three months of receipt.
 - **Equipment. Data users** must ensure that individual monitors do not show confidential information to passers-by, and that they log off from their PC when it is left unattended.
 - **Working away from the school premises** – paper documents should not be removed from site. The exceptions to this rule include meetings with other agencies (for example, local authorities, police, social or health care) and for safeguarding purposes. Where paper documents

are removed from site, it is the employees responsibility to ensure they are secure at all times. Loss of paper documents is considered a data breach and must be reported immediately.

- **Working away from the school premises – electronic working.** Staff must not use external storage devices, including USB or similar hard drives. Staff must not download data to personal devices. Where staff are working offsite they should take precautions to ensure data is kept secure and confidential, this includes avoiding any unauthorised viewing of data on devices. The loss of a device must be reported immediately.
- **Document printing-** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers or left out of lockable storage to prevent unauthorised access.
- **Technical and organisational security controls** include:
 - multi-factor authentication for user accounts
 - single sign-on through centrally managed identities
 - role-based access and least-privilege permissions
 - managed Trust devices with security policies applied centrally
 - encryption of data in transit and at rest
 - automatic screen locking and secure authentication requirements
 - anti-malware, web filtering and email threat protection
 - security updates and patch management
 - monitoring and logging of account and system activity
 - secure, tested backups and recovery arrangements
 - regular review and removal of dormant, unnecessary or former-user accounts
 - phishing awareness and data protection training
 - controlled processes for approving new systems and applications
 - supplier security and data protection due diligence
 - data protection impact assessments where processing may create increased risk
 - documented procedures for reporting, managing and learning from security incidents and personal data breaches.

13.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14 Personal data breaches

14.1 The Trust recognises that a breach of **personal data** could happen, despite our policies, procedures, and measures in place to protect **personal data**, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm to individuals.

14.2 The Trust has a personal data breach procedure, and this must be followed in relation to any actual or suspected breach of **personal data**. All breaches must be logged on to the SchoolPro platform immediately.

15 Disclosure and sharing of personal information

- 15.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the local authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.
- 15.2 The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.
- 15.3 Where necessary, we will enter into a data sharing agreement to help facilitate the safe sharing of **personal data**.
- 15.4 In some circumstances we will not share safeguarding information. Please refer to our child protection policy.

16 Data processors

- 16.1 We contract with various organisations who provide services to the Trust. These include people, companies, and systems that process personal data on our behalf and under our instruction.
- 16.2 In order that these services can be provided effectively, we are required to transfer **personal data** of **data subjects** to these **data processors**.
- 16.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.
- 16.4 Contracts with **data processors** will comply with data protection legislation and contain explicit obligations on the **data processor** to ensure compliance with the data protection legislation, and compliance with the rights of **data subjects**.

17 Images and videos

- 17.1 Parents and others attending Trust events are allowed to take photographs and videos of those events for personal and domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.
- 17.2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

- 17.3 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.
- 17.4 Whenever a pupil begins their attendance at the Trust, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. Images and videos of pupils may be required for safeguarding, assessment, and learning purposes and we will not seek consent for the taking and use of these images. However, as a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

18 Video Surveillance

- 18.1 We use CCTV in various locations around our school sites to ensure it remains safe. We will adhere to the ICO's guidance for the use of CCTV when we do so.
- 18.2 CCTV imagery will be retained only as long as is necessary, for a minimum period of 5 calendar days and a maximum period of 6 months unless it is footage which relates to an incident under review.
- 18.3 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
- 18.4 Access to recorded images will be restricted to the those staff authorised to view them, and will not be made more widely available.
- 18.5 Staff should not seek to delete, alter or tamper with CCTV data, especially where this relates to an incident under view.
- 18.6 Any enquiries about the CCTV system should be directed to the DOP.

19 Biometric Data

- 19.1 The Trust does not operate a biometric recognition system and no biometric data for pupils is used or stored by the Trust or its schools.
- 19.2 Before we are able to obtain the Biometric Data of staff, we are required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

19.3 For staff, written consent will be obtained at the commencement of their position within the Trust and shall continue to be effective unless an objection in writing to the processing of your Biometric Data is received from the individual.

20 Complaints

20.1 Data subjects have the right to make a complaint to the Trust if they consider we have not complied with data protection legislation. Any complaints relating to data protection must be directed to our DPO.

20.2 When dealing with complaints relating to data protection, we shall:

- Acknowledge receipt of the complaint within 30 days of the date on which the complaint is received by the Trust.
- Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate.
- Inform the complainant about progress of the complaint; and
- Inform the complainant of the outcome of the complaint.

21 Disposal of data

21.1 Personal data is stored and disposed of in accordance with the retention schedule, see appendix 2.

21.2 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

22 Training

22.1 All staff, volunteers and contractors are provided with data protection training as part of their induction process and then annually thereafter.

22.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

23 Complaints

23.1 Data subjects have the right to make a complaint to the Trust if they consider we have not complied with data protection legislation. Any complaints relating to data protection must be directed to our DPO.

23.2 When dealing with complaints relating to data protection, we shall:

- Acknowledge receipt of the complaint within 30 days of the date on which the complaint is received by the Trust.
- Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate.
- Inform the complainant about progress of the complaint; and
- Inform the complainant of the outcome of the complaint.

24 Changes to this policy

24.1 The DPO is responsible for monitoring and reviewing this policy, which will be reviewed **every 2 years**, or sooner where required.

25 Social responsibility statement:

25.1 Liberty Academy Trust acts with integrity and accountability in all aspects of its operations. We strive to make a positive impact on our students, staff, communities, and the environment by promoting equity, sustainability, and ethical practices. Our commitment to social responsibility underpins every decision we make, ensuring that we contribute to the well-being of society while fostering an inclusive and respectful educational culture.

Appendix 1

DEFINITIONS

Term	Definition
Biometric Data	is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting
Biometric Recognition System	is a system that operates automatically (electronically) and : • Obtains or records information about a person's physical or behavioural characteristics or features; and • Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data

	protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or Biometric Data
Staff	Includes, any individual employed by Trust such as staff, agency workers and consultants, and those who volunteer in any capacity including Trustees, Members, local governors and parent helpers

Appendix 2

Data Retention Schedule