DATA PROTECTION POLICY

Last review date	September 2025
Date approved by the Trust Board	September 2025
Date for next review	September 2026

Document Control

Document version numbering will follow the following format. Whole numbers for approved versions, eg 1.0, 2.0, 3.0 etc. Decimals will be used to represent the current working draft version, eg 1.1, 1.2, 1.3 etc. For example, when writing a procedural document for the first time the initial draft will be version 0.1.

The table below provides details of the changes made to this document, to inform those reviewing and approving the document.

Document Edition	Section	Details of Change
2.0	Introduction	Six Es updated to 3.
2.1	All	Full review of the policy
3.0	All	Approved by Trust Board 6 March 2024
3.1	Subject Access Requests	Updated April 2024 in line with DfE guidance
3.2	All	Updated by COO in line with new Dfe guidance (changes highlighted in yellow)
4.0	All	Approved by Trust Board October 2024
5.0	All	Approved by Trust Board September 2025

Table of Contents

Introduction 4

Aims 4

Legislation and Guidance 4

Definitions 5

The Data Controller 6

Roles and Responsibilities 6

- Board of Trustees 6
- Data Protection Officer 6
- Headteacher 6
- All staff 6

Data Protection Principles 7

Collecting Personal Data 7

- Lawfulness, fairness and transparency 7
- Limitation, minimisation and accuracy 8

Sharing Personal Data 9

Subject access requests and other rights of individuals 9

- Subject access requests 9
- Children and subject access requests 10
- Responding to subject access requests 10
- Other data protection rights of the individual 11

Parental Requests to see the Educational Record 11

Biometric Recognition Systems 11

CCTV 12

Photographs and Videos 12

Artificial intelligence (AI) 12

Data Protection by Design and Default 13

Data Security and Storage of Records 13

Disposal of Records 14

Personal Data Breaches 14

Training 14

Monitoring Arrangements 14

Appendix 2: Data Breach Investigation Report 18

Introduction

The Leading Edge Academies Partnership (the 'Trust') is a team of school leaders that aim to be Leading Edge and pioneering in their approach to education and wellbeing. We are a growing family of like-minded schools that offer a values based education to the communities we serve and welcome staff, students, parents/carers and volunteers from all different ethnic groups and backgrounds.

The term 'Trust Community' includes all staff, trustees, governors, pupils, parents/carers, volunteers and visitors.

We are a values based Trust, which means all actions are guided by our three 'Es' as follows:

- **Excellence** – 'Outstanding quality'
- **Evolution** – 'Continuous change'
- **Equity** – 'Fairness and social justice'

This policy is based on the value of **'Equity'**

Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, parents and carers, members, trustees, governors, visitors, and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and Guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. In a school, examples of personal data include: • identity details (for example, a name, title or role) • contact details (for example, an address (physical or email) or a telephone number) • information about pupil behaviour and attendance • assessment and exam results • staff recruitment information • staff contracts • staff development reviews • staff and pupil references It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
Special categories of personal data	Special category data is personal data that's considered more sensitive and given greater protection in law. Special category data includes: • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade-union membership • genetic information • biometric information (for example, a fingerprint) • health matters (for example, medical information) • sexual matters or sexual orientation In a school, it would be best practice to also treat as special category data any personal data about: • a safeguarding matter • pupils in receipt of pupil premium • pupils with special educational needs and disability (SEND) • children in need (CIN) • children looked after by a local authority (CLA)

Criminal offence data	Criminal offence data is personal data that's treated in a similarly sensitive way to special category data. It records criminal convictions and offences or related security measures. Criminal offence data includes: • the alleged committing of an offence • the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data assets	Schools hold personal data in several forms. These are collectively known as its data assets. Data assets comprise: • data items – single pieces of information • data item groups – data items about the same process • data sets – collections of related data that can be manipulated as a unit by a computer • systems – administrative software • system groups – the larger systems housing administrative software
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach	A data breach is a security incident that results in personal data a school holds being: • lost or stolen • destroyed without consent • changed without consent • accessed by someone without permission Data breaches can be deliberate or accidental. A breach is about more than just losing personal data.

The Data Controller

Leading Edge Academies Partnership processes personal data relating to parents, pupils, staff, trustees, visitors and others, and therefore is a data controller.

Leading Edge Academies Partnership is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and Responsibilities

This policy applies to **all staff** employed by the Trust and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Leading Edge Academies Partnership complies with all relevant data protection obligations.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on the Leading Edge Academies Partnership data protection issues.

The DPO is also the first point of contact for individuals whose data the academy processes and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Mr David Teasdale, telephone number 01736 688442.

In addition to the DPO, each Trust school appoints an Information Management Lead who will support the DPO to maintain local oversight and to manage any DPO issues or concerns. The name of the individual in each school will be available from the Headteacher or DPO.

Headteacher and senior leaders

Senior leaders are accountable for:

- deciding how the school uses technology and maintains its security
- deciding what data is shared and how
- setting school policies for the use of data and technology

- understanding what UK GDPR and the Data Protection Act covers and getting advice from the data protection officer, as appropriate
- assuring governors and trustees that the school has the right policies and procedures in place
- making sure any contracts with third-party data processors cover the relevant areas of data protection
- making sure staff receive training on data protection annually

Staff training on data protection should include training on specific school processes such as:

- personal data breach reporting processes
- the escalation of information rights requests

All staff

All staff should be aware of what:

- personal data is
- 'processing' means
- their duties are in handling personal information
- the processes are for using personal information
- is permitted usage of that data
- the risks are if data gets into the wrong hands
- their responsibilities are when recognising and responding to a personal data breach
- the process is for recognising and escalating information rights requests

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

Staff who collect, store or view personal data are responsible for:

- making sure they have a legitimate need to process the data
- checking that any data they store is needed to carry out necessary tasks
- identifying any risks
- understanding the governance arrangements that oversee the management of risks

Data Protection Principles

Our Trust must comply with the UK GDPR data protection principles.

The principles for the processing of personal data are:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability

This policy sets out how Leading Edge Academies Partnership aims to comply with these principles.

Collecting Personal Data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- **consent** – where this basis is the most appropriate and we are able to give the individual concerned a real choice in our use of their data
- **contract** – where our use of the data is necessary for a contract the Trust or school has or will have with the individual concerned
- **legal obligation** – where our use of the data is necessary to permit the Trust or school to comply with the law
- **vital interests** – where our use of the data is necessary to protect an individual's life
- **public interest** – where our use of the data is necessary to permit the Trust or school to carry out a task in the public interest or our official functions, and that task or function has a clear basis in law
- **legitimate interests** – where our use of the data is necessary for the Trust, school's or a third party's legitimate interests (unless there's a good reason to protect the individual's personal data that overrides those legitimate interests)

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law.

- **explicit consent** – the accessing or processing of this personal data has the written consent of the individual concerned
- **employment, social security or social protection** – it is necessary for one of these 3 stated purposes and authorised by law
- **vital interests** – it is necessary to protect an individual's life

- **not-for-profit body** – it is necessary for the legitimate internal-only purposes of a membership body with a political, philosophical, religious or trade-union aim
- **manifestly made public** – it relates to personal data the individual has themselves deliberately made public
- **legal claims or judicial acts** – it is necessary for a legal case or required by a court of law
- **substantial public interest** – there is a relevant basis in UK law and one of 23 specific public interest conditions has been met
- **health or social care** – it is necessary for the provision of healthcare or treatment, or of social care, and there is a basis in law
- **public health** – it is necessary for reasons of public interest, and there is a basis in law
- **archiving, research and statistics** – it is necessary for reasons of public interest, and there is a basis in law

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights.**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

Sharing Personal Data

We will not normally share personal data with anyone else, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- In order to keep children safe and make sure they get the support they need; we must share information with other schools and agencies. We may not ask for consent to share personal information for the purposes of safeguarding a child.
- If a pupil moves to another school, we will transfer their records to the new school.
- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law.
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service.
- We will also share personal data with law enforcement and government bodies where we are legally required to do so.
- We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
- Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school or Trust holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form to anyone that works in the organisation. Once an individual has made a request, they cannot be asked to change the format they made the request in. An

individual does not have to call their request a SAR and staff should be aware of a potential SAR when dealing with complaints or any reference to Data Protection legislation.

We may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If an employee receives a subject access request, they must immediately forward it to the school Information Management Lead and the DPO.

An individual can make a request for personal data that relates to:

- Themselves
- Someone they have personal responsibility for
- Someone they have permission to act on behalf of

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our primary schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our secondary schools may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

When a child of any age submits a SAR, the member of staff dealing with the request should consider whether they can understand the information they will receive in response to their request.

They should not respond directly to the child if they believe they:

- do not have the maturity or competence to act independently
- have a health condition that limits their understanding
- have given consent for a representative or someone with parental responsibility to act on their behalf

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification (this will always be the case if the individual is not known to the school).
- If the individual is asking for someone else's information, they will need to provide the individuals ID and evidence that they have the authority to act on the individuals behalf.
- May contact the individual via phone to confirm the request was made.

- May contact the individual for clarification of what specific information they are looking for
- Will respond without delay and within 1 calendar month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

Receiving a SAR during the school holidays

If a SAR is received on the last day of the school term, or during the school holidays, the school must still respond within one calendar month. Education settings cannot extend a SAR response because it is the school holidays.

If the school are unable to meet the legal deadline of one calendar month, they should let the requester know as soon as possible.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
    - The information has previously been provided by the school or the individual already hass access to the information. We will explain this to the individual making the request and evidence that the information has already been accessed or seen.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek the right to enforce their subject access request right through the courts.

Manifestly unfounded SARs

A manifestly unfounded SAR is when an individual submits multiple SARs with malicious intentions.

For example, a parent submits a SAR every week with the intention of harassing a staff member following an earlier disagreement. The parent offers to withdraw their SAR for personal benefit.

Before refusing to comply with a request on these grounds it is important to show the reasons why it is believed that a request is not genuine.

A request might not be genuine if:

- it includes details of an intention to cause disruption
- it targets an employee with unproven accusations

Manifestly excessive SARs

A manifestly excessive SAR means that the effort and cost of collecting the information makes responding to the request unreasonable or disproportionate.

This is not an easy assessment to make. We will consider all the circumstances of the request before making a decision. The ICO provides comprehensive guidance about what factors need to be considered.

Notifying a requester about a refused SAR

We will notify a requester that their SAR has been refused within one calendar month from the day they made the SAR. We will also include the reason for the refusal. The requester will be given details about how to complain to the ICO or seek a judicial review.

Redacting information

Depending on what an individual asks for, we may need to remove some information. This process is known as redacting.

We will redact personal information that identifies anyone other than the person the SAR is about. This is known as removing third party information.

In some cases, we may need to release third party information. This decision must be made on a case-by-case basis, and we will record any decisions we make about releasing third party data.

We may need to redact information about:

- other pupils
- other parents
- staff

When redacting identifiable information, we will make sure that redactions cannot be undone.

Individuals may ask to see CCTV images of themselves or their child. CCTV images contain personal information. Images of other people appearing in CCTV images will be redacted, for example by blurring.

A SAR entitles a person to access their own personal information but does not entitle them to access full documents. We may extract personal information from a document to include in the SAR response, and provide context of where the information is held.

We will keep a copy of unredacted and redacted versions of information in case of review.

Information that is no longer available

In some cases, an individual might ask for information we no longer hold. We will respond by telling them the information is no longer held by the organisation.

We will refer the requester to our data retention policy or privacy notice.

Complaints about a SAR response

A SAR response letter must include the following information:

- organisation contact regarding the response, usually the data protection officer
- details on how to complain to the ICO
- acknowledgement of their right to seek judicial remedy
- acknowledgement of their other data protection rights such as the right to have their information deleted or changed

If an individual is unhappy with their SAR response, we can offer them the chance for their case to be reviewed.

If an individual remains unhappy with the school or Trust's response, they can complain to the ICO. The ICO will consider the complaint and contact the school or Trust for further information or to provide advice as appropriate.

When an organisation processes a SAR, they should anticipate any future challenge or a formal ICO complaint. Completing a case review record while handling a SAR, which details what decisions have been made and why, may serve as a useful tool when responding to complaints.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time or stop processing their personal information (right to object verbally or in writing).
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
- Be notified of a data breach (in certain circumstances).
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).
- Remove their personal information or record.

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO and local Information Management lead. A response to the request must be provided within one calendar month. If the case is complex, this can be extended to two calendar months.

Access to Data

- Individuals may submit an information rights request relating to personal data either verbally or in writing, including through social media.
- Information rights requests only apply to the personal data the organisation holds when it receives the request.
- Individuals have the right to request changes or restrictions to personal information, but a school is not obliged to make changes to data in certain circumstances.

Parental Requests to see the Educational Record

As an academy trust, parents, or those with parental responsibility, do not have an automatic parental right of access to their child's educational record. However, it is the Trust's policy to allow parental access to their child's data upon receipt of a written request.

Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the Trust's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the Trust's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the academy will delete any relevant data already captured.

CCTV

We may use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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.

Any enquiries about the CCTV system should be directed to the Headteacher.

Photographs and Videos

As part of the Trust's activities, we may take photographs and record images of individuals within our schools.

We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Uses may include:

- Within each school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns

- Online on school websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Employees, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Trust 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, the Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in Appendix 1.

Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school offices.
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites.

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

Disposal of Records

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.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. This will include taking steps to ensure that all staff are able to recognize a personal data breach and how to formally report it to the school Information Management Lead.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on any school's website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

Training

All employees, trustees and governors are provided with data protection training as part of their induction process.

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

Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full board of trustees.

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the employee/trustee/governor/volunteer or data processor must immediately notify the local Information Management Lead and the DPO by telephone, email, or face to face.
- The Information Management Lead will carry out an initial investigation into the breach, using the Data Breach Investigation Report Form (Appendix 2). The DPO will review the initial findings and, if necessary, will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been,
    - Made available to unauthorised people.
- Employees (and others, where applicable), will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation (although a subsequent disciplinary investigation may follow if deemed necessary).
- If a breach has occurred, the DPO will alert the Headteacher, CEO and the Chair of Trustees (if necessary).
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant employees or data processors where necessary. The DPO will take external advice where required (e.g. from IT providers). Actions relevant to specific data types are set out at the end of this procedure.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.
- The DPO will work out whether the breach must be reported to the ICO using the ICOs self-assessment tool.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the LE-Information Management Team which can be accessed by school Information Management Leads and the DPO.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible: §

      The categories and approximate number of individuals concerned.

      § The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO.
  - A description of the likely consequences of the personal data breach.
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).
- Records of all breaches will be stored in the LE – Information Management Team.

The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

Employees/trustees/governors/volunteers who receive personal data sent in error must alert the sender, school Information Management Lead and the DPO as soon as they become aware of the error.

If the sender is unavailable or cannot recall the email for any reason, the Information Management Lead or the DPO will ask the IT department to recall it.

In any cases where the recall is unsuccessful, the Information Management Lead or the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

The Information Management Lead or the DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

The Information Management Lead or the DPO will ask the IT department to carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Appendix 2: Data Breach Investigation Report

This template outlines the key information to be gathered during an investigation into a data breach. Once the investigation has been carried out, the completed form should be sent to the Trust DPO.

The Trust DPO is David Teasdale (COO), dteasdale@leadingedgeacademies.org, 01736 688442.

Summary

School	
Date of Breach	
Date reported to MAT	

Details of Breach

Provide **details of the breach**, what happened and how?
Who was responsible?

How many people were affected? When were they informed?

Who had access to the data?

Who investigated the breach?

Impact of Breach

Outline of the impact of the breach.

Measures taken to support the affected person.

Learning from Breach

Outline the learning from the breach and any process changes that will be made to avoid reoccurrence.

To be completed by the DPO:

Breach or Near Miss?

Reported to Trustees (Y/N)? Date of report (if reported)

Reported to ICO (Y/N)? Date of report (if reported)

Findings of ICO and feedback.

Further action (if required) (include owner and review date).