Data Protection Policy

Date	22nd July 2024
Written By	Director of Governance and Compliance
Approve by Executive	TBC
Review Date	July 2026

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. Data protection principles 4
6. Fair and lawful processing 4
7. Processing for limited purposes 7
8. Notifying data subjects 7
9. Adequate, relevant and non-excessive processing 8
10. Accurate data 8
11. Timely processing 8
12. Processing in line with data subjects' rights 8
13. Data security 11
14. Data Protection Impact Assessments 12
15. Disclosure and sharing of personal information 12
16. Data Processors 12
17. Images and Videos 13
18. Video Surveillane 13
19. Biometric Data 14
20. Changes to this policy 14

Appendix 1 – Definitions 15
Appendix 2 – Data retention and destruction 17

Key Information

Data protection officer (DPO): Chris Rossiter

Contact details: dpo@libertytrust.org.uk

References to external sources:

- Department for Education's Data Protection in Schools toolkit.
- IRMS 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** and failure to comply with this policy may result in those fines being applied.

1.4 All members of our **workforce** must comply with this policy when processing **personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

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 has been designed in accordance with the Department for Education's Data Protection in Schools toolkit.

2.3 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.

2.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.5 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 The data controller

4.1 The Academy Trust processes personal data relating to parents, pupils, staff, volunteers (including non-executives), visitors and others, and therefore is a data controller. The Academy Trust is registered with the ICO and will renew this registration annually, along with relevant Data Protection fee as legally required.

5 Roles and responsibilities

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

5.1 Liberty Academy Trust Board

The Trust Board has overall responsibility for ensuring that our academies comply with all relevant data protection obligations.

5.2 Data Protection Officer

As a Trust, we are required to appoint a Data Protection Officer ("DPO").

The DPO is responsible for 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.

The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

The DPO must be consulted when planning projects and other activities which may involve the collection or processing of additional personal data.

5.3 Principals

The Principal acts as the representative of the data controller on a day-to day basis in our schools.

5.4 IT and data team

LAT's IT manager, system administrators and technicians are responsible for ensuring all data systems are protected from unauthorised access and against the accidental loss of, or damage to, **personal data**. Only staff are granted access to data in line with the Trust's schedule of access.

Where the Trust uses third-party platforms and applications stipulations must be made in accordance with this policy and included in any procurement criteria, contract or service level agreement.

Third-party DPIAs must be recorded in the Trust's register of processing activity.

5.5 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the academy of any changes to their personal data, such as a change of address and contact details
- 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 or not they have a lawful basis to collect and or store/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, including the use of a new data processor and the upload of data to third party companies such as new learning platforms requiring students to log in
    - If they need help with any contracts or sharing personal data with third parties
    - If they need to apply a UK GDPR principle to processing data.

6 Data protection principles

6.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

- **Processed** fairly and lawfully and transparently in relation to the **data subject**;
- **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept for any longer than is necessary for the purpose; and
- **Processed** securely using appropriate technical and organisational measures.

6.2 **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.

6.3 We will comply with these principles in relation to any **processing** of **personal data** by the Trust, including its schools.

7 Fair and lawful processing

7.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

7.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

- that the **personal data** is being **processed**;
- why the **personal data** is being **processed**;
- what the lawful basis is for that **processing** (see below);
- whether the **personal data** will be shared, and if so with whom;
- the period for which the **personal data** will be held;
- the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and
- the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

7.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

7.4 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, (e.g the Education Act 2011);
- where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and
- where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data**.

7.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. 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 consent of the **data subject** to the **processing** of their **special category personal data**.

7.6 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.

7.7 If any **data user** is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

Vital Interests

7.8 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 in a position 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. However, the DPO must be notified of any such incidents within 24 hours after the initial incident.

Consent

7.9 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.

7.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

7.11 When pupils and or our staff 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.

7.12 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.

7.13 We will generally seek consent directly from a pupil who has reached the age of 13 years, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

7.14 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.

7.15 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.

7.16 The DPO must always be consulted in relation to any consent form before consent is obtained.

7.17 A record must always be kept of any consent, including how it was obtained and when.

8 Processing for limited purposes

8.1 In the course of our activities as a Trust, we may collect and **process** the **personal data** set out in our Register of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of staff).

8.2 We will only process **personal data** for the specific purposes set out in our Register of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

9 Notifying data subjects

9.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

- our identity and contact details as **Data Controller** and those of the DPO;
- the purpose or purposes and legal basis for which we intend to **process** that **personal data**;
- the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;
- whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;
- the period for which their **personal data** will be stored, by reference to Retention and Destruction guidelines;
- the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and
- the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

9.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

10 Adequate, relevant and non-excessive processing

We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

11 Accurate data

11.1 We will ensure that **personal data** we hold is accurate and kept up to date.

11.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

11.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

12 Timely processing

12.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

12.2 We shall seek to comply with the rights exercised by **data subjects** as soon as possible and within legal time limits. However, there may be instances where due to circumstances outside of the Trust's control this may not be possible e.g. where the School or Trust has been closed or is only partially operable. In such circumstances data subjects till be notified and provided details about the reason for the delay and when a response can reasonably be expected.

13 Processing in line with data subjects' rights

13.1 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.

The Right of Access to Personal Data

13.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure.

The Right to Object

13.3 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

13.4 An objection to **processing** does not have to be complied in certain circumstances where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

13.5 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

13.6 In respect of direct marketing any objection to **processing** must be complied with.

13.7 The Trust is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

13.8 If a **data subject** informs the Trust that **personal data** held about them by the Trust is inaccurate or incomplete then we will consider that request and provide a response within one month.

13.9 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.

13.10 We may determine that any changes proposed by the **data subject** should not be made. If this is the case then 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 Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

13.11 **Data subjects** have a right to "block" or suppress the **processing** of personal data. This means that the Trust can continue to hold the **personal data** but not do anything else with it.

13.12 The Trust must restrict the **processing** of **personal data**:

- Where it is in the process of considering a request for **personal data** to be rectified (see above);
- Where the Trust is in the process of considering an objection to processing by a **data subject**;
- Where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**; and
- Where the Trust no longer needs the **personal data** but the **data subject** has asked the Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust.

13.13 If the Trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

13.14 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

13.15 **Data subjects** have a right to have **personal data** about them held by the Trust erased only in the following circumstances:

- Where the **personal data** is no longer necessary for the purpose for which it was originally collected;
- When a **data subject** withdraws consent – which will apply only where the Trust is relying on the individuals consent to the **processing** in the first place;
- When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;
- Where the **processing** of the **personal data** is otherwise unlawful;
- When it is necessary to erase the personal data to comply with a legal obligation; and

13.16 The Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

- To exercise the right of freedom of expression or information;
- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, research or statistical purposes; or
- In relation to a legal claim.

13.17 If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

13.18 The DPO must be consulted in relation to requests under this right.

Right to Data Portability

13.19 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to other organisation.

13.20 if such a request is made then the DPO must be consulted.

14 Subject Access Requests

14.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the 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, but we will 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
- Date range of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

14.2 Children and subject access requests

Those with parental responsibility have the right to access their child's educational records under separate legislation. This can typically be provided quicker than a full subject access request. Should you wish to exercise this right please see section 15 below.

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 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 academy 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 by the academy Principal.

The Principal must not refuse a request from a child with Special Educational Needs or Disability (SEND) solely on the basis of his or her SEND characteristic – any

such request must be treated according to the individual circumstances of the child.

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 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
- Provide the information digitially unless you request otherwise
- 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.

We will not disclose information 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
- Would contravene exemptions as established in the Act, for example if disclosure would adversely affect the rights and freedoms of others or jeopardise police investigations into any alleged offence(s)

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account the time and cost of fulfilling the request and 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 may subsequently seek to enforce their subject access right through the courts.

15 Parental requests to see the educational record

15.1 Parents, or those with parental responsibility, have a right under this policy to access to their child's educational record (which includes most information about a pupil) within 30 school days of receipt of a written request.

If the request is for a copy of the educational record, the Trust may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

16 Freedom of Information requests

16.1 **LAT's Responsibilities**

LAT understands its responsibilities in relation to FOIA (2000) and is committed to applying them.

16.2 Publication Scheme

LAT has adopted the ICO's model publication scheme for state-funded schools in England. Further details on what the Trust provides access to can be found on the Trust's website.

Right of Access

Any person can make a freedom of information request for information that the Trust holds. The request must be in writing (which can include email) and state the requestor's name and correspondence address (including email address). It should clearly describe the information being requested with enough detail to enable us to identify and locate the information. Where a request is for environmental information which can be released under the EIR, this request can be made verbally. We would request however that any request is made in writing.

Requests should be addressed to the DPO.

If the freedom of information request is sent to the Trust seeking information from the Trust, a response will be provided as soon as possible but in any event within 20 working days (which excluded public holidays) following the date of receipt. However, where the request has been sent to a School within the Trust seeking information from the School, the School will seek to respond within 20 school days (or 60 working days, if shorter) for information provided under FOIA. Where information is to be provided under the EIR this will be provided within 20 working days. A School day is a day when there is a session at which pupils are in attendance at school.

Where the original request is not clear and we are required to seek further clarity from you, the time for responding to your request will cease until we receive a further response from you. In the event that we do not receive a further response or the clarification requested within 2 months of our request for clarification we will assume you no longer wish to pursue your enquiry and close the matter down.

16.3 Exemptions

Requested information may not be provided if one of the following applies:

- LAT does not hold the information;
- There is a relevant exemption available;

- The request is above the cost limit (being £450 or 18 hours of a staff member's time).
- Where additional clarity or a fee has been requested but has not been provided in the time specified; or
- The request is considered vexatious or repeated

The exemptions that may be relevant depend on the request that has been made, but common exemptions include data protection, prejudice to the effective conduct of public affairs and information intended for future publication. There are other exemptions that may also be relevant, details of which can be found on the ICO website at Freedom of information and Environmental Information Regulations | ICO

We will inform you if one or more of these apply in any decision notice. Where the cost limit applies, we will explain how to refine the request to bring it within the cost limit and why the costs limit has been exceeded.

16.4 Internal Review

Where a requester is not happy with the response to a freedom of information request that has been made, they will be entitled to ask for an internal review of the decision. The internal review must be requested within two months of the decision notice being sent. The internal review will usually be dealt with by someone more senior than the member of staff that provided the initial response. A requester will in most cases receive the outcome of the internal review within 20 working / school days dependent on whether the review is of a Trust or a school response.

Where a requester wishes to have an internal review of an EIR request, this should be requested in writing within 40 working days of any breach of a requirement under the EIR. Once an internal review request is received, we aim to conclude the review and communicate the outcome of this within 20 working days.

If a requester is still not happy with the response following an internal review, they can complain to the Information Commissioner using the following link: FOI and EIR complaints | ICO.

17 Data security

17.1 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**.

17.2 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.

17.3 Security procedures include:

- **Entry controls**. Any unauthorised person seen in entry-controlled areas should be reported to the DPO immediately.
- **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

- **Monitoring and tracking.** The IT team routinely monitor access to data and systems, including electronic devices such as computers, printers, and photocopiers, and software including email. Systems are in place to automatically track data access and sharing, including externally. Queries may be made to staff directly when such activity is identified and staff are required to responsed as necessary.

- **Methods of disposal**. See section 23 below.

- **Data encryption.** Data shared externally should be encrypted. This may be achieved using a third-party platform, such as Egress. If encryption is unavailable, then staff should use password protected documents or electronic links to documents where data can be monitored.

- **Equipment**. Data users must ensure that individual monitors do not show confidential information to passers-by and that they always log off from their PC when it is left unattended.

- **Working away from Trust premises – paper documents.** Data users must not keep paper records and or remove them from Trust premises. Where this is unavoidable paper documents should be stored and disposed of as per this policy, including section 23.

- **Working away from the school premises – electronic working**. Data users should observe the security procedures above. Devices must be password protected and data users should be aware of their surroundings when using personal data on screens.

- **Document printing**. Print logs are routinely monitored by the IT team. Documents containing **personal data** must be collected immediately from printers and not left on photocopiers. Printed matter should not be removed from the school site.

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

18 Data Protection Impact Assessments

18.1 The Trust takes data protection very seriously, and 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.

18.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. 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 the way that we intend to do so.

18.3 The Trust will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

18.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

19 Disclosure and sharing of personal information

19.1 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, Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

19.2 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.

19.3 In some circumstances we will not share safeguarding information. Please refer to our Safeguarding Policy.

19.4 Further detail is provided in our Data Protection Impact Assessment and Register of Processing Activities.

20 Data Processors

20.1 Our suppliers or contractors need data to enable us to provide services to our staff and pupils, for example in relation to IT.

20.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

20.3 **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.

20.4 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**

20.5 A copy of the Data Protection Impact Assessment of each supplier or contractors must be given to the Trust and held centrally for inspection.

21 Data Protection Impact Assessment

21.1 A Data Protection Impact Assessment (DPIA) is a process to help LAT identify and minimise the data protection risks of a project.

21.2 DPIAs are mandatory when processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. A DPIA must be completed prior to data processing.

21.3 DPIAs may be used when working with a single data processing operation, however, in accordance with Article 35(1) similar processing activities can also be incorporated into a single assessment where they present similar high risks.

21.4 As such this DPIA will consider processing activities and the risks they represent across LAT because many of these activities are similar in nature, scope, context, and purpose.

21.5 In future, DPIAs will be carried out on new technology and software where they are used to generate, store or otherwise process personal data. In this instance LAT staff should obtain the existing DPIA from the technology provider and incorporate any high level risks into the attached risk register.

22 Images and Videos

22.1 LAT's staff, volunteers and contractors are forbidden from taking images or videos of any pupil on their personal devices. Using personal devices in this way will result in disciplinary action.

22.2 Parents and others attending Trust events are allowed to take photographs and videos of those events for 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.

22.3 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.

22.4 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.

22.5 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. 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.

22.6 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. We will not use images or videos of pupils for any purpose where we do not have consent.

23 Video Surveillance

23.1 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.

23.2 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.

23.3 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.

23.4 Access to recorded images will be restricted to the those staff authorised to view them, and will not be made more widely available.

23.5 Staff should not seek to delete, alter or tamper with CCTV data, especially where this relates to an incident under view.

23.6 Any enquiries about the CCTV system should be directed to the DOP.

24 Biometric Data

24.1 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.

24.2 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.

24.3 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.

24.4 Further information about this can be found in our Notification of Intention to Process Pupil's Biometric Information and our Privacy Notices.

25 Disposal of data

25.1 Personal data is stored and disposed of in accordance with the IRMS Schools Toolkit.

25.2 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.

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.

25.3 The Freedom of Information Act (2000) requires the Trust to maintain a list of records that have been destroyed and who authorised their destruction. All data should be destroyed immediately once approved.

26 Personal data breaches

26.1 The academy will make all reasonable endeavours to ensure that there are no personal data breaches.

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

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

27 Training

27.1 All staff, volunteers and contractors are provided with data protection training as part of their induction process.

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

28 Changes to this policy

28.1 The DPO is responsible for monitoring and reviewing this policy, which will be reviewed **every 2 years** and shared with the full Board of Trustees.

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