



Leodis
Academies
Trust

DATA PROTECTION POLICY

Policy Details	
Document Name:	Leodis Academies Trust Data Protection Policy
Version Number:	V5.2
Effective From:	1 June 2025
Owner(s):	Trust Data Protection Officer
Approved by:	Trust Board
Next review date:	1 June 2026
Consultation:	COO, CEO Principal, Principals, HR Manager, DSLs

Document History			
Version	Date	Author	Note of Revisions
1.0	May 2018	DPO	
2.0	February 2019	DPO/Business Manager	Additional of 'police' and health professionals and agencies including the NHS' that staff and student data may b shared with.
3.0	May 2019	DPO	Amendments to Subject Access Request in Section 9.
4.0	May 2020	DPO	Addition of section 17.13 to cover procedure of Third-Party Data Breaches and section 9.13 which relates to a new procedure document.
5.0	September 2024	DPO	Revisions made to convert into Trust Format and make reporting process clearer. All sections updated. Rebranded, reformatted and dates updated. Section 2.6: Reference to radicalisation and terrorism concerns added.
5.1	Nov 2024	DPO	Updates made to the change name of the Local Governing Board/ Local Advisory Board to Local Committees/Local Committees (Advisory) to reflect the changes to the roles and responsibilities

			outlined in the Academy Trust Governance Guide 2024.
5.2	June 2025	DPO	Updated to reflect Trust AI Policy and checks with DfE Data Protection Guidance

CONTENTS

Section	Title	Page No.
1.	INTRODUCTION	2
2.	AIMS AN SCOPE OF THE POLICY	2
3.	STATUTORY GUIDANCE	2
4.	LINKS WITH OTHER TRUST POLICIES	3
5.	ROLES AND RESPONSIBILITIES	3
6.	DATA PROTECTION PRINCIPLES	5
7.	FAIR AND LAWFUL PROCESSING	5
8.	PROCESSING FOR LIMITED PURPOSES	8
9	NOTIFYING DATA SUBJECTS	8
10.	ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING	8
11.	ACCURATE DATA	9
12.	TIMELY PROCESSING	9
13.	PROCESSING IN LINE WITH DATA SUBJECT RIGHTS	9
14.	DATA SECURITY	12
15.	DATA PROTECTION IMPACT ASSESSMENTS	12
16.	DISCLOSURE AND SHARING OF PERSONAL INFORMATION	13
17.	DATA PROCESSORS	13
18.	IMAGES AND VIDEOS	13
19.	VIDEO SURVEILLANCE	14
20.	BIOMETRIC DATA	14
	ANNEX - DEFINITIONS	15

1. INTRODUCTION

- 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, 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 **staff** must comply with this policy when processing **personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.
- 1.5 Where members of our **staff** have a specific responsibility in connection with **processing**, such as capturing consent, reporting a Personal Data Breach, or conducting a Data Protection Impact Assessment as referred to in this Data Protection Policy or otherwise, then they must comply with the related policies and privacy guidelines.
- 1.6 There has been consideration of rapidly developing AI implications throughout this policy.

2. AIMS AND SCOPE OF THE POLICY

- 2.1 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.
- 2.2 The types of **personal data** that we may be required to handle include information about pupils, parents, our **staff**, 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**').
- 2.3 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3. STATUTORY GUIDANCE

- 3.1 This policy is written with consideration to:
 - General Data Protection Regulation ((EU)2016/679) ('UK **GDPR**')
 - Department for Education (DfE) Data Protection Toolkit [Data protection in schools - Guidance - GOV.UK](#)
 - Information Commissioner's Office (ICO) guidance [Information Commissioner's Office](#)
 - DfE AI in Education Guidance [Generative artificial intelligence \(AI\) in education - GOV.UK](#)
 - IRMS Schools Toolkit [IRMS Schools Toolkit - Information and Records Management Society](#)

4. LINKS WITH OTHER TRUST POLICIES

4.1 A number of Academy / Trust policies and procedure documents make reference to Data Protection including:

- 4.1.1 Trust Safeguarding and Child Protection Policy
- 4.1.2 Artificial Intelligence Policy
- 4.1.3 Whistleblowing Policy
- 4.1.4 Processing of Special Categories of Personal Data and Criminal Office Data Policy
- 4.1.5 Freedom of Information Policy
- 4.1.6 CCTV Policy
- 4.1.7 Privacy Notices
- 4.1.8 Acceptable Usage Agreements
- 4.1.9 Trust Retention Schedule
- 4.1.10 Schedule of Processing Activities
- 4.1.11 Subject Access Request Procedures
- 4.1.12 Notification of Intention to Process Pupil's Biometric Information

4.2 This list of policies is not exhaustive and does not replace the general requirements documented in all Trust and Academy policies and procedures.

4.3 Where legal obligations or statutory guidance are updated, the Trust will follow the most up to date legal obligations which may differ from information stated in this policy. The policy will be updated as soon as practicably possible.

5. ROLES AND RESPONSIBILITIES

5.1 The Trustees of Leodis Academies Trust

The Trustees have overall responsibility for:

- 5.1.1 Annual review of the policy.
- 5.1.2 Annual report of the effectiveness of the policy.
- 5.1.3 Approving amendments to the policy.

5.2 The CEO Principal

The CEO Principal has overall responsibility for:

- 5.2.1 Maintaining and operating the policy.
- 5.2.2 Ensuring that this policy is communicated Trust Wide.
- 5.2.3 To work with the Trust Data Protection Officer in line with this policy.
- 5.2.4 Ensuring that this policy is followed by the Trust Central Team.

5.3 Trust Data Protection Officer

- 5.3.1 As a Trust, we are required to appoint a Data Protection Officer ("DPO"). The named Trust DPO is **Katy Stringer**
- 5.3.2 The DPO and Data Protection Team can be contacted at **dpo@leodis.org.uk**
- 5.3.3 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.

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

5.4 **Local Committee (LC)**

- 5.4.1 The LC and Principal of each Academy are responsible for the implementation of the Data Protection Policy within their Academy.
- 5.4.2 The LC is responsible for supporting senior leaders promoting the policy locally.

5.5 **Academy Principal**

- 5.5.1 The Academy Principal is responsible for implementing and communicating the Data Protection Policy to all staff within their Academy
- 5.5.2 The Principal is responsible for ensuring staff are informed of any changes made.
- 5.5.3 The Principal must
- Ensure that all data protection matters relating to their Academy are managed in line with this Policy.
 - Maintain a record of concerns raised and the outcomes (but in a form that does not endanger confidentiality) and will report as necessary to the Trust Data Protection Officer, Governors and Trustees as required.
 - Liaise with the Trust Data Protection Officer as required, seeking advice and support for data protection matters as required
 - Maintain confidentiality.
- 5.5.4 The Principal will appoint staff to be the Academy Data Protection Lead(s)

5.6 **Academy Data Protection Lead**

An Academy Data Protection Lead will

- 5.6.1 Work with the Principal to ensure all aspects of Data Protection policies and procedures, including this retentions schedule are implemented at the Academy.
- 5.6.2 Undertake investigations in line with Trust Policies and Procedures without any undue delay as directed by the DPO and/or CEO Principal or Academy Principal.
- 5.6.3 Maintain confidentiality.

5.7 **All Staff**

Staff must:

- 5.7.1 Ensure personal data is processed in line with this Policy
- 5.7.2 Ensure AI policy and guidelines are followed
- 5.7.3 Ensure data security measures are followed at all times
- 5.7.4 Raise issues of concern responsibly in line with this Policy.
- 5.7.5 Participate in any investigation deemed necessary and as a result maintain confidentiality.
- 5.7.6 Understand their data protection responsibilities, which are part of their employment or role, and be aware that sanctions will be applied if these provisions are breached.
- 5.7.7 Ensure annual training is completed in line with Trust requirements

5.8 Contractors, Parents and Visitors

5.8.1 This Data Protection Policy refers to how the Trust manages data in relation to all data subjects. For any enquiries about how this affects your personal data as a contractor, parent or visitor, please refer to our Privacy Notices.

6. DATA PROTECTION PRINCIPLES

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

6.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**.

6.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes.

6.1.3 Adequate, relevant, and not excessive for the purpose.

6.1.4 Accurate and up to date.

6.1.5 Not kept for any longer than is necessary for the purpose; and

6.1.6 **Processed** securely using appropriate technical and organisational measures.

6.2 **Personal Data** must also.

6.2.1 be **processed** in line with **data subjects'** rights.

6.2.2 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.

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:

7.2.1 that the **personal data** is being **processed**;

7.2.2 why the **personal data** is being **processed**;

7.2.3 what the lawful basis is for that **processing** (see below);

7.2.4 whether the **personal data** will be shared, and if so with whom.

7.2.5 the period for which the **personal data** will be held;

- 7.2.6 the existence of the **data subject's** rights in relation to the **processing** of that personal data; and
- 7.2.7 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:
 - 7.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;
 - 7.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);
 - 7.4.3 where the law otherwise allows us to **process** the **personal data**, or we are carrying out a task in the public interest;
 - 7.4.4 where we are pursuing legitimate interests, (or these are being pursued by a third party), for purposes where they are not overridden because the **processing** prejudices the interests or fundamental rights and freedoms of **data subjects**; and
 - 7.4.5 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:
 - 7.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;
 - 7.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
 - 7.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
 - 7.5.4 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.

7.8 Vital Interests

- 7.8.1 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, but is not limited to, 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 immediately. Should this be necessary retrospective documentation will be completed.

7.9 Consent

- 7.9.1 Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.
- 7.9.2 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.
- 7.9.3 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.
- 7.9.4 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.
- 7.9.5 When required, for example a Subject Access Request, we will seek consent directly from a pupil who has reached the age of 13. We recognise, however, that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.
- 7.9.6 If consent is required for any other **processing of personal data** of any **data subject**, then the form of this consent must:
- 7.9.6.1** Inform the **data subject** of exactly what we intend to do with their **personal data**.
 - 7.9.6.2** Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
 - 7.9.6.3** Inform the **data subject** of how they can withdraw their consent.
- 7.9.7 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.
- 7.9.8 Consent may need to be refreshed where we may need to process the **Personal Data** for different and incompatible purpose which was not disclosed when the consent was first considered by the **Data Subject**.
- 7.9.9 The DPO must always be consulted in relation to any consent form before consent is obtained.

- 7.9.10 A record must always be kept of any consent/withdrawal of 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 **Schedule 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 our **staff**).
- 8.2 We will only process **personal data** for the specific purposes set out in our **Schedule 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:
- 9.1.1 our identity and contact details as **Data Controller** and those of the DPO.
 - 9.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**.
 - 9.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**.
 - 9.1.4 whether the **personal data** will be transferred outside United Kingdom and if so the safeguards in place.
 - 9.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy.
 - 9.1.6 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
 - 9.1.7 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

- 10.1 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 will maintain retention policies and procedures to ensure **Personal Data** is deleted after an appropriate time, unless a law requires that the data is to be kept for a minimum time.
- 12.3 We shall seek to comply with the rights exercised by **data subjects** as set out in section 12 below 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 will 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 SUBJECT RIGHTS

- 13.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:
 - 13.1.1 request access to any **personal data** we hold about them.
 - 13.1.2 **object** to the **processing** of their **personal data**, including the right to object to direct marketing.
 - 13.1.3 **have** inaccurate or incomplete **personal data** about them rectified.
 - 13.1.4 **restrict processing** of their **personal data**.
 - 13.1.5 **have** **personal data** we hold about them erased.
 - 13.1.6 **have** their **personal data** transferred; and
 - 13.1.7 object to the making of decisions about them by automated means.
- 13.2 **The Right of Access to Personal Data**
 - 13.2.1 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the Trust's Subject Access Request Procedure.
- 13.3 **The Right to Object**
 - 13.3.1 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 based on a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

- 13.3.2 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.
- 13.3.3 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.
- 13.3.4 In respect of direct marketing any objection to **processing** must be complied with.
- 13.3.5 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.

13.4 The Right to Rectification

- 13.4.1 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.
- 13.4.2 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.
- 13.4.3 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.

13.5 The Right to Restrict Processing

- 13.5.1 **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.
- 13.5.2 The Trust must restrict the **processing** of **personal data**:
 - 13.5.2.1 Where it is in the process of considering a request for **personal data** to be rectified (see above).
 - 13.5.2.2 Where the Trust is in the process of considering an objection to processing by a **data subject**.
 - 13.5.2.3 Where the **processing** is unlawful, but the **data subject** has asked the Trust not to delete the **personal data**; and
 - 13.5.2.4 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.
- 13.5.3 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.
- 13.5.4 The DPO must be consulted in relation to requests under this right.

13.6 The Right to Be Forgotten

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

13.6.1.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected.

13.6.1.2 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.

13.6.1.3 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.

13.6.1.4 Where the processing of the **personal data** is otherwise unlawful.

13.6.1.5 When it is necessary to erase the personal data to comply with a legal obligation; and

13.6.2 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:

13.6.2.1 To exercise the right of freedom of expression or information.

13.6.2.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law.

13.6.2.3 For public health purposes in the public interest.

13.6.2.4 For archiving purposes in the public interest, research, or statistical purposes; or

13.6.2.5 In relation to a legal claim.

13.6.3 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.

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

13.7 Right to Data Portability

13.7.1 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 another organisation.

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

14. DATA SECURITY

- 14.1 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**.
- 14.2 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.
- 14.3 Security procedures include:
- 14.3.1 **Entry controls.** Any stranger without an authorised lanyard seen in entry-controlled areas should be reported to the **Principal or Senior member of staff immediately**.
 - 14.3.2 **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.)
 - 14.3.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets and the Trust Asset Disposal procedure.
 - 14.3.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock/log off from their electronic devices when it is left unattended.
 - 14.3.5 **Working away from the school premises – paper documents** should be kept to a minimum to prevent data loss. Documents should be kept securely when not in use and not be worked on in places where others can access the information
 - 14.3.6 **Working away from the school premises – electronic working.** The Trust has Multi-Function Authentication (MFA) in place for the use of school devices away from the premises. Work should be completed in places where others cannot access the information or listen into confidential calls. The use of USB devices is prohibited. Equipment should be locked away when not in use.
 - 14.3.7 **Document printing** - Documents containing **personal data** must be collected immediately from printers and not left on photocopiers. The Trust has secure access procedures in place to ensure most printing can only be collected using a staff ID card.
- 14.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

15. DATA PROTECTION IMPACT ASSESSMENTS

- 15.1 The Trust takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.
- 15.2 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. This will be recorded on the **Trust Schedule of Processing Activities**.

- 15.3 The Trust will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.
- 15.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

16. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

- 16.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.
- 16.2 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.
- 16.3 In some circumstances we will not share safeguarding information. Please refer to the Safeguarding and Child Protection Policy.
- 16.4 Further detail is provided in our **Privacy Notices** and **Schedule of Processing Activities**.

17. DATA PROCESSORS

- 17.1 We contract with various organisations who provide services to the Trust, both for curriculum purposes, administering Academy / Trust business and contracts of employment.
- 17.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data** subjects to these **data processors**.
- 17.3 **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.
- 17.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.
- 17.5 The **Schedule of Processing Activities** captures this information.

18. IMAGES AND VIDEOS

- 18.1 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.
- 18.2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.
- 18.3 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

- 18.4 As a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.
- 18.5 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.

19. VIDEO SURVEILLANCE

- 19.1 The Trust operates CCTV system in the Academies. Please refer to the Trust CCTV Policy.

20. BIOMETRIC DATA

- 20.1 The Trust operates a biometric recognition system for the purposes of:
- 20.1.1 payment of dinner monies at Woodkirk Academy
- 20.2 Before we are able to obtain the Biometric Data of pupils, 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.
- 20.3 For pupils under the age of 18 years, the Academy will notify each parent of that pupil (that the we have the contact details for and is able to contact) prior to them commencing their education at the school of the use of our Biometric Recognition System. The Academy will then obtain the written consent of one of the pupil's parents before obtaining any Biometric Data.
- 20.4 In the event that written consent cannot be obtained from a parent, or any parent objects in writing or the pupil objects or refuses to participate in the processing of their Biometric Data, the Academy will not process the pupil's Biometric Data and will provide the following alternative means of accessing the above service.
- 20.5 Where this Academy provides the pupil with a card to access the catering function and make payment. It is the responsibility of the pupil to ensure this card is kept safe.
- 20.6 Further information about this can be found in our **Notification of Intention to Process Pupil's Biometric Information** and our **Privacy Notices**.

ANNEX A

Term	Definitions
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	<p>is a system that operates automatically (electronically) and:</p> <p>Obtains or records information about a person's physical or behavioural characteristics or features; and</p> <p>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</p>
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 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 staff (including Trustees, 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, sexual orientation or genetic or Biometric Data
Staff	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Trustees / Members/ Governors / parent helpers