



DATA PROTECTION POLICY

Including Biometric Information



Contents

1. Intent.....	3
2. Key Contacts and Related Policies	4
3. Definitions.....	5
4. Legal Framework and Guidance.....	7
5. Roles and Responsibilities.....	8
6. Data Protection Principles.....	11
7. Lawful, Fair and Transparent Processing.....	12
8. Collecting and Using Personal Data.....	15
9. Sharing Data, Processors and International Transfers	17
10. Individual Rights and Subject Access Requests.....	20
11. Children's Information and Parental Requests	24
12. Biometrics, CCTV, Photographs and Videos.....	27
13. Artificial Intelligence and Automated Decision-Making.....	30
14. Data Protection by Design, DPIAs and Accountability Records	32
15. Security, Retention and Disposal	34
16. Personal Data Breaches.....	36
17. Data Protection Complaints.....	38
18. Training, Monitoring and Review.....	40

1. Intent

- 1.1** Endeavour Learning Trust (ELT) is committed to protecting the personal data it processes and respecting the information rights of individuals.
- 1.2** The purpose of this policy is to establish a clear and consistent approach to data protection across the Trust. It sets out the principles, responsibilities and controls which apply when personal data is collected, accessed, recorded, used, amended, stored, shared, retained or disposed of.
- 1.3** This policy applies to Endeavour Learning Trust and all academies within the Trust. It covers all personal data processed by or on behalf of the Trust, whether held electronically, on paper or in any other format.
- 1.4** The Trust processes personal data relating to pupils, parents and carers, employees, workers, job applicants, members, trustees, local governors, volunteers, visitors, contractors, suppliers and other individuals with whom the Trust has contact.
- 1.5** This policy applies to members, trustees, local governors, employees, agency workers, volunteers, contractors and any other person who processes personal data on behalf of the Trust.
- 1.6** Everyone covered by this policy must comply with it and with any related policies, procedures, standards and guidance relevant to their role. Failure to do so may result in action under the relevant disciplinary, contractual or governance arrangements.
- 1.7** This policy does not form part of any employee's contract of employment. The Trust will review and update it where required to reflect changes in legislation, regulatory guidance, technology or the Trust's processing activities.

2. Key Contacts and Related Policies

Endeavour Learning Trust's Data Protection Officer

- 2.1** The Trust-level contact for data protection matters is the Data Protection Officer (DPO). Their contact details are listed below:

Name	Emma Cockburn-Hyde
Role	Head of Governance, Compliance and Risk (DPO)
Email	dataprotection@endeavourlearning.org

School-Level Contact

- 2.2** Each ELT academy (school) identifies a Data Protection Lead to act as the first point of contact for school-level data protection queries.

Contact Routes

- 2.3** The following contact routes should be used:

Matter	Contact Route
Data protection advice and general enquiries	The relevant school-level Data Protection Lead or the Trust's Data Protection Officer
Subject access requests and other information rights requests	The relevant academy Data Protection Lead for academy-held information, or the relevant central service lead for centrally held information, supported by the Data Protection Officer
Data protection complaints	The Trust's Data Protection Officer
Actual or suspected personal data breaches	The relevant school-level Data Protection Lead and the Trust's Data Protection Officer, using the Trust's breach-reporting process
Freedom of Information and Environmental Information requests	The Trust's Governance Team (dataprotection@endeavourlearning.org)
CCTV enquiries	The relevant contact identified within the CCTV Policy

Related Policies and Procedures

- 2.4** This policy should be read alongside the following related policies, procedures and notices:

- Subject Access Request Procedure
- CCTV Policy
- Freedom of Information Policy
- Freedom of Information Publication Scheme
- Records Management and Retention Schedules Policy
- Governance Privacy Notice
- Parents and Pupils (Under 13) Privacy Notice
- Pupils (Aged 13 and Over) Privacy Notice
- Staff Privacy Notice
- Visitors, Contractors and Suppliers Privacy Notice
- Complaints Procedure
- Child Protection and Safeguarding Policy

3. Definitions

3.1 The definitions in the table below apply throughout this policy.

Term	Definition
Data Protection Legislation	The UK General Data Protection Regulation, the Data Protection Act 2018, the Data (Use and Access) Act 2025 insofar as it amends applicable data protection law, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any other applicable data protection or privacy legislation, including any amendments or replacement legislation in force from time to time.
Personal Data	Any information relating to an identified or identifiable living individual. An individual may be identified directly or indirectly, including through a name, identification number, location data, online identifier or other characteristic. Personal data may include factual information or an opinion about an individual.
Special Category Personal Data	Personal data requiring additional protection because it reveals or concerns an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to uniquely identify them, health, sex life or sexual orientation.
Criminal Offence Data	Personal data relating to criminal convictions, offences, allegations, proceedings, sentences or related security measures. Criminal offence data is subject to additional legal protections but is not special category personal data.
Processing	Any operation or set of operations performed on personal data, whether or not by automated means. This includes collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, sharing, alignment, combination, restriction, erasure and destruction.
Data Subject	The identified or identifiable living individual to whom personal data relates.
Data Controller	The person, public authority, organisation or other body which, alone or jointly with others, determines the purposes and means of processing personal data.
Data Processor	A person, organisation or other body which processes personal data on behalf of, and under the instructions of, a Controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.
Consent	A freely given, specific, informed and unambiguous indication of a Data Subject's wishes, given through a statement or clear affirmative action, signifying agreement to the processing of their personal data.
Pseudonymisation	Processing personal data so it cannot be attributed to a particular individual without additional information, where that additional

	information is kept separately and protected by appropriate technical and organisational measures.
Biometric data	Personal data resulting from specific technical processing relating to an individual's physical, physiological or behavioural characteristics which enables or confirms their unique identification. Examples include fingerprints and facial recognition data.
Automated Decision-making	Making a decision solely through automated processing, without meaningful human involvement. A significant automated decision is one which produces a legal or similarly significant effect on an individual.
Profiling	Automated processing of personal data to evaluate or predict aspects relating to an individual, such as their performance, health, preferences, interests, reliability, behaviour, location or movements.
Data Protection Impact Assessment (DPIA)	A documented assessment used to identify and reduce the data protection risks of processing which is likely to result in a high risk to individuals' rights and freedoms.
Subject Access Request (SAR)	A request made by or on behalf of an individual for access to their personal data and the supplementary information to which they are entitled under Data Protection Legislation.
Data Protection Lead (DPL)	The person identified by an academy to coordinate day-to-day data protection activity and act as its local point of contact. The DPL supports the Trust's compliance arrangements but does not replace the statutory responsibilities of the Data Protection Officer or the Trust as Data Controller.

4. Legal Framework and Guidance

- 4.1** The Trust will process personal data in accordance with applicable Data Protection Legislation, including:
- [The UK General Data Protection Regulation \(UK GDPR\)](#)
 - [the Data Protection Act 2018](#)
 - [the Data \(Use and Access\) Act 2025](#)
 - The Privacy and Electronic Communications (EC Directive) Regulations 2003, where applicable
 - [the Protection of Freedoms Act 2012](#)
- 4.2** This policy also has regard to relevant guidance, codes of practice and resources published by the Information Commissioner's Office, including guidance concerning:
- [UK data protection legislation](#)
 - individual rights and subject access requests
 - processing children's information
 - data sharing
 - artificial intelligence and automated decision-making
 - data protection impact assessments
 - personal data breaches
 - [video surveillance, including CCTV](#)
- 4.3** The Trust also has regard to relevant Department for Education guidance and resources, including:
- [Data Protection in Schools](#)
 - [Protection of Children's Biometric Information in Schools](#)
 - [Generative Artificial Intelligence \(AI\) and Data Protection in Schools](#)
 - the Department for Education's model privacy notices
- 4.4** The Trust will also comply with the data protection provisions contained within its funding agreements and Articles of Association.
- 4.5** References to legislation and guidance include any amendments, replacements or updated versions in force from time to time. Where legislation or statutory guidance changes, the current requirements will apply pending formal review of this policy.

5. Roles and Responsibilities

The Data Controller

- 5.1** Endeavour Learning Trust is the Data Controller for the personal data processed by the Trust and its academies. The Trust determines why and how personal data is processed.
- 5.2** The Trust is registered with the Information Commissioner's Office and maintains its registration as legally required. The Trust's registration number is ZA462273.

Trust Board

- 5.3** The Trust Board has collective and overall accountability for the Trust's compliance with Data Protection Legislation.
- 5.4** The Trust Board is responsible for:
- approving this policy
 - ensuring that data protection risks receive appropriate scrutiny
 - appointing and, where necessary, removing the Data Protection Officer in accordance with the Scheme of Delegation
 - ensuring that the Data Protection Officer has sufficient independence, authority, access and resources
 - considering advice and assurance provided by the Data Protection Officer
 - receiving an annual report on data protection compliance

Audit and Risk Committee

- 5.5** The Audit and Risk Committee supports the Trust Board by:
- reviewing this policy and recommending it to the Trust Board for approval
 - reviewing assurance about the effectiveness of the Trust's data protection arrangements
 - considering significant risks, incidents and audit findings
 - monitoring agreed actions and reporting relevant matters to the Trust Board
 - making recommendations concerning the appointment or removal of the Data Protection Officer

Chief Executive

- 5.6** The Chief Executive has operational accountability for implementing this policy and monitoring compliance across the Trust. This includes ensuring that appropriate resources, systems and controls are in place, senior leaders understand their responsibilities, the Data Protection Officer is involved in relevant matters and the Trust Board receives appropriate assurance.

Data Protection Officer

- 5.7** The Data Protection Officer acts independently when performing their statutory duties and reports directly to the Trust Board as the Trust's highest management level. They must not receive instructions about how to perform those duties or be dismissed or penalised for performing them. Any additional duties must not create a conflict of interest.

5.8 The Data Protection Officer is responsible for:

- Informing and advising the Trust Board, senior leaders and staff about their obligations under Data Protection Legislation
- monitoring compliance with Data Protection Legislation and this policy
- advising on and monitoring Data Protection Impact Assessments
- supporting the development and review of data protection policies, procedures, privacy notices and training
- advising on information rights requests, Personal Data Breaches, complaints, data sharing, contracts and international transfers
- cooperating with and acting as a contact point for the Information Commissioner's Office and Data Subjects
- undertaking or commissioning audits and compliance reviews
- reporting directly to the Trust Board at least annually and sooner where a significant matter requires its attention

5.9 Responsibility for compliance remains with the Trust as Data Controller. The Data Protection Officer advises and monitors the Trust but is not personally responsible for the Trust's compliance.

Executive Team and Central Team Leads

5.10 Members of the Executive Team and central service leads are responsible for implementing this policy within their areas of responsibility. They must ensure that staff receive appropriate training, access to personal data is controlled, contracts and new processing activities receive appropriate review, centrally held information rights requests are managed and identified risks or incidents are addressed.

Headteachers

5.11 In accordance with the Scheme of Delegation, Headteachers are responsible for implementing this policy within their academies. They must nominate and support an academy Data Protection Lead, ensure staff understand their responsibilities and ensure that local requests, incidents and compliance concerns are managed within the required timescales.

Academy Data Protection Leads

5.12 Each academy's Data Protection Lead coordinates day-to-day data protection activity within the academy and acts as the first local point of contact.

5.13 The Data Protection Lead is responsible for:

- supporting staff to apply this policy and related procedures
- receiving, managing and completing Subject Access Requests and other information rights requests relating to the academy
- coordinating searches, reviews, redactions and responses in accordance with the Trust's procedures
- receiving and escalating actual or suspected Personal Data Breaches
- supporting local privacy notices, accountability records, retention arrangements and training
- seeking advice from the Data Protection Officer on complex requests, exemptions, complaints, high-risk processing and other matters requiring specialist advice

The Trust's ICT Team

5.14 The ICT Team is responsible for:

- implementing appropriate technical security and access controls
- supporting the secure operation, backup and recovery of Trust systems
- responding to cyber security and personal data incidents
- supporting information searches and retrieval
- advising on the security of systems, suppliers and processors

All Staff and Other Authorised Users

5.15 All staff and other authorised users of personal data must:

- comply with this policy and related procedures
- access and use personal data only where authorised and necessary for their role
- keep personal data accurate, secure and confidential
- use approved systems, devices and methods for storing or sharing personal data
- refer information rights requests and data protection complaints promptly
- report actual or suspected Personal Data Breaches immediately
- complete required training and follow retention and secure disposal requirements
- seek advice from the relevant academy Data Protection Lead or the Trust's Data Protection Officer when unsure

6. Data Protection Principles

- 6.1** The UK GDPR sets out seven data protection principles. The Trust must apply these principles whenever it processes personal data.
- 6.2** Personal data must be:
- processed lawfully, fairly and transparently
 - collected for specified, explicit and legitimate purposes, and not processed further in a manner incompatible with those purposes
 - adequate, relevant and limited to what is necessary for the purposes for which it is processed
 - accurate and, where necessary, kept up to date, with reasonable steps taken to correct or erase inaccurate personal data without delay
 - kept in a form which identifies individuals for no longer than is necessary
 - processed securely, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
 - managed in accordance with the accountability principle
- 6.3** Under the accountability principle, the Trust is responsible for complying with these principles and must be able to demonstrate its compliance through appropriate policies, procedures, records, controls and assurance arrangements.
- 6.4** The remaining sections of this policy explain how the Trust applies these principles.

7. Lawful, Fair and Transparent Processing

Lawful Basis

- 7.1** The Trust will only process personal data where it has identified a lawful basis for doing so.
- 7.2** Before processing begins, the Trust will identify and document:
- the purpose of the processing
 - the lawful basis relied upon
 - why the processing is necessary
 - any additional condition required for special category or criminal offence data
- 7.3** The lawful bases available under the UK GDPR are:
- **Consent:** where the individual has given valid consent for a specific purpose
 - **Contract:** where processing is necessary to perform a contract with the individual or take steps requested before entering into a contract
 - **Legal Obligation:** where processing is necessary to comply with the law
 - **Vital Interests:** where processing is necessary to protect someone's life
 - public task, where processing is necessary to perform a task in the public interest or exercise an official function with a clear basis in law
 - **Recognised Legitimate Interest:** where processing is necessary for a purpose covered by one of the recognised legitimate interest conditions set out in Annex 1 to the UK GDPR
 - **Legitimate Interests:** where processing is necessary for the legitimate interests of the Trust or a third party and those interests are not overridden by the individual's rights and interests
- 7.4** No lawful basis takes priority over another. The Trust will select the basis which most closely reflects the purpose and circumstances of the processing. Where a lawful basis requires the processing to be necessary, the Trust will consider whether the purpose reasonably and proportionately requires the use of personal data.
- 7.5** As a public authority, the Trust will not rely on recognised legitimate interest or legitimate interests when processing personal data to perform its public tasks. The Trust will only consider these bases for activities outside its public tasks where the relevant legal requirements are met.

Special Category and Criminal Offence Data

- 7.6** When processing special category personal data, the Trust will identify and document:
- a lawful basis under Article 6 of the UK GDPR
 - a condition for processing under Article 9 of the UK GDPR and, where required, Schedule 1 of the Data Protection Act 2018
- 7.7** When required by the Data Protection Act 2018, the Trust will maintain an Appropriate Policy Document explaining its procedures for complying with the data protection principles and its arrangements for retaining and deleting the information.
- 7.8** When processing criminal offence data, the Trust will identify and document a lawful basis under Article 6 of the UK GDPR and either official authority or an appropriate condition under Schedule 1 of the Data Protection Act 2018.

Consent

- 7.9** The Trust will only rely on consent where the individual has a genuine choice and control over the use of their personal data. Consent must be:
- freely given
 - specific
 - informed
 - unambiguous
 - given through a clear statement or positive action
- 7.10** Silence, inactivity or pre-ticked boxes do not constitute valid consent. The Trust will obtain explicit consent where this is required for processing special category personal data.
- 7.11** The Trust will record how and when consent was obtained. Individuals must be able to withdraw consent as easily as they gave it. Withdrawal does not affect the lawfulness of processing undertaken before consent was withdrawn.
- 7.12** Requirements relating to children's consent are set out in Section 11. Requirements relating to consent for biometrics, photographs and videos are set out in Section 12.

Fairness and Transparency

- 7.13** The Trust will process personal data in ways individuals would reasonably expect. It will consider the effect of the processing on their rights and interests and will not mislead them about how their personal data is collected or used.
- 7.14** The Trust will provide privacy information which is concise, accessible and written in clear language. Information intended for children will be presented in a form they are likely to understand.
- 7.15** Where personal data is collected directly from an individual, the relevant privacy information will be provided when the data is collected.
- 7.16** Where personal data is obtained from another source, the relevant privacy information will be provided within one month, at the first communication with the individual or before the first disclosure, whichever is earliest, unless an exemption applies.
- 7.17** Privacy information will include, where relevant:
- the identity and contact details of the Trust and its Data Protection Officer
 - the purposes of the processing and the lawful bases relied upon
 - the categories and sources of personal data
 - any legitimate interests relied upon
 - the recipients or categories of recipients
 - details of international transfers and safeguards
 - the applicable retention periods
 - the individual's information rights
 - the right to withdraw consent where consent is relied upon
 - whether providing the information is a statutory or contractual requirement and the consequences of not providing it
 - details of automated decision-making and profiling
 - the right to raise a complaint with the Trust and the Information Commissioner's Office

- 7.18** The Trust will review and update its privacy information when its processing activities or legal obligations change.
- 7.19** Staff must consult the relevant Data Protection Lead or the Data Protection Officer before beginning new processing where the correct lawful basis or additional condition is unclear.

8. Collecting and Using Personal Data

Collecting Personal Data

- 8.1** The Trust will only collect personal data which it needs for a specified purpose and for which it has identified an appropriate lawful basis.
- 8.2** Personal data will be collected:
- directly from the individual
 - from a parent, carer or authorised representative
 - from another school, academy trust, local authority, government department or public body
 - from other lawful sources relevant to the specified purpose
- 8.3** The Trust will use appropriate and secure methods to collect personal data. The privacy information required under Section Seven will be provided unless an exemption applies.
- 8.4** Staff must not collect personal data because it might be useful in the future. Collection must relate to an identified and documented purpose.

Purpose Limitation

- 8.5** The Trust will clearly identify and record the purposes for which it collects and uses personal data. These purposes will be recorded within the Trust's records of processing activities and relevant privacy notices.
- 8.6** Personal data will only be used for:
- the purpose for which it was collected
 - a compatible purpose permitted under Data Protection Legislation
 - a new purpose for which the requirements in this section have been met

Using Personal Data for a New Purpose

- 8.7** Before using personal data for a new purpose, the Trust will:
- identify and document the new purpose
 - determine whether the new purpose is compatible with the original purpose
 - identify an appropriate lawful basis
 - identify any additional condition required for special category or criminal offence data
 - update the relevant records of processing activities
 - update the relevant privacy information and inform affected individuals where required
 - complete a Data Protection Impact Assessment where the processing is likely to result in a high risk to individuals
- 8.8** When assessing whether a new purpose is compatible with the original purpose, the Trust will consider:
- any link between the original and new purposes
 - the circumstances in which the personal data was collected
 - the Trust's relationship with the individual and their reasonable expectations
 - the nature and sensitivity of the personal data
 - the possible consequences for the individual

- the safeguards applied to the processing

8.9 The Trust will treat a new purpose as compatible where the UK GDPR expressly provides for this and the relevant statutory conditions are met. This includes specified processing connected with:

- safeguarding vulnerable individuals
- responding to emergencies
- preventing, detecting or investigating crime
- protecting vital interests
- complying with legal obligations
- protecting public security
- responding to certain requests from bodies performing public tasks
- archiving in the public interest, scientific or historical research or statistical purposes

8.10 Where personal data was originally collected on the basis of consent, the Trust will obtain consent for the new purpose unless Data Protection Legislation expressly permits the proposed use without further consent.

Data Minimisation

8.11 The Trust will ensure that the personal data it collects and uses is:

- sufficient to fulfil the specified purpose
- relevant to the specified purpose
- limited to the minimum amount reasonably required

8.12 The Trust will review forms, systems and processing activities to ensure that unnecessary personal data is not requested, recorded or retained. Particular care will be taken when collecting special category or criminal offence data.

Accuracy

8.13 The Trust will take reasonable steps to ensure that personal data is accurate and not misleading. Where necessary for the purpose of the processing, personal data will be kept up to date.

8.14 The Trust will record the source and status of personal data where this is relevant to its accuracy and use.

8.15 Where personal data is found to be inaccurate or misleading, the Trust will correct or erase it without delay. Where required, the Trust will notify recipients to whom the inaccurate information was disclosed.

8.16 Records will distinguish clearly between fact and opinion. Where an opinion is recorded, the record should identify whose opinion it is and provide sufficient context to understand it.

8.17 A record is not inaccurate solely because it records an event which was later reversed, corrected or disputed. The Trust will ensure that the record includes the subsequent correction, decision, outcome or challenge where this is needed to prevent the record from being misleading.

8.18 Individuals have the right to request correction of inaccurate personal data. Further information about this right is provided in Section 10.

9. Sharing Data, Processors and International Transfers

Sharing Personal Data

- 9.1** The Trust will only share personal data where the sharing is lawful, fair, necessary, proportionate and secure.
- 9.2** Before sharing personal data, the Trust will consider:
- the purpose of the sharing
 - the lawful basis relied upon
 - any additional condition required for special category or criminal offence data
 - whether the recipient has a lawful and legitimate need for the information
 - the minimum personal data required
 - whether the sharing is within the individual's reasonable expectations
 - the security of the proposed method of sharing
 - whether a Data Protection Impact Assessment or data sharing agreement is required
- 9.3** The Trust will verify the identity and authority of the recipient before disclosing personal data. The information shared will be limited to what the recipient needs for the specified purpose.
- 9.4** Consent is not required where another lawful basis applies. The Trust will share personal data without consent where the law requires or permits the sharing, including where necessary to:
- safeguard a child or vulnerable individual
 - protect someone's vital interests
 - respond to an emergency
 - prevent, detect or investigate crime
 - comply with a court order or another legal obligation
 - perform a task in the public interest
- 9.5** Data protection concerns must not prevent necessary and proportionate information sharing for safeguarding purposes. Staff must record the reasons for significant sharing decisions, including decisions not to share where this affects safeguarding or welfare.
- 9.6** Personal data will be shared using approved and secure methods. Staff must not use personal email accounts, unapproved applications or other unauthorised methods to share Trust information.
- 9.7** Regular, systematic or higher-risk sharing arrangements will be documented in a data sharing agreement where appropriate. The agreement will set out:
- the parties and their respective roles
 - the purpose and lawful basis for sharing
 - the personal data involved
 - how the information will be used
 - security and access arrangements
 - retention and deletion arrangements
 - arrangements for information rights requests, complaints and personal data breaches
 - review and termination arrangements
- 9.8** A data sharing agreement does not provide a lawful basis for sharing. The Trust must identify the lawful basis separately.

- 9.9** Where the Trust and another organisation jointly determine the purposes and means of processing, they will establish a transparent written arrangement setting out their respective responsibilities as joint controllers.

Data Processors

- 9.10** The Trust will only appoint processors which provide sufficient guarantees that they will protect personal data and comply with Data Protection Legislation.

- 9.11** Before appointing a processor, the Trust will assess matters including:

- the processor's experience and reliability
- technical and organisational security measures
- access controls and staff confidentiality arrangements
- arrangements for personal data breaches
- use of sub-processors
- data storage and access locations
- international transfers
- retention, deletion and return of personal data
- independent assurance, certifications or audit findings

- 9.12** Processing must be governed by a written contract or other legally binding arrangement meeting Article 28 of the UK GDPR. The arrangement will state:

- the subject matter and duration of the processing
- the nature and purpose of the processing
- the types of personal data and categories of Data Subjects
- the Trust's rights and obligations

- 9.13** The arrangement will require the processor to:

- process personal data only on the Trust's documented instructions, including instructions concerning international transfers, unless otherwise required by law
- ensure authorised personnel are subject to appropriate confidentiality requirements
- implement appropriate technical and organisational security measures
- appoint a sub-processor only with the Trust's prior written authorisation and under an arrangement providing equivalent data protection obligations
- assist the Trust with information rights requests, security obligations, Personal Data Breaches, Data Protection Impact Assessments and prior consultation with the Information Commissioner's Office
- at the Trust's choice, return or delete all personal data at the end of the arrangement and delete existing copies unless the law requires their storage
- provide the information and access required for audits, inspections and compliance checks
- inform the Trust immediately if, in the processor's opinion, an instruction breaches Data Protection Legislation

- 9.14** The Trust remains responsible for personal data processed on its behalf and will monitor processors throughout the contractual relationship.

- 9.15** Staff must not appoint a processor, introduce a service or upload personal data to an external system without completing the Trust's required approval, procurement, security and data protection checks.

International Transfers

- 9.16** Personal data must not be transferred outside the UK unless the transfer complies with Data Protection Legislation and has been approved through the Trust's relevant processes.
- 9.17** An international transfer includes remote access, technical support, cloud hosting or onward transfer where personal data is made available to a separate organisation outside the UK.
- 9.18** A restricted international transfer will only take place where one of the following applies:
- the destination is covered by UK adequacy regulations
 - appropriate safeguards are in place, such as the UK International Data Transfer Agreement, the UK Addendum to approved EU Standard Contractual Clauses or approved Binding Corporate Rules
 - a specific legal exception applies to the transfer
- 9.19** Where appropriate safeguards are relied upon, the Trust will complete and document a transfer risk assessment, applying the statutory data protection test, and introduce any additional protections required.
- 9.20** Legal exceptions for international transfers will only be used in limited circumstances and will not be relied upon for routine or repeated transfers without appropriate review.
- 9.21** Staff must consult the Data Protection Officer before establishing a new international transfer or materially changing an existing transfer.

10. Individual Rights and Subject Access Requests

10.1 Requests relating to information held by an academy will normally be coordinated by that academy's Data Protection Lead. Requests relating to information held centrally will normally be coordinated by the relevant central service lead. Where information is held across academy and central systems, the Data Protection Officer will confirm who will coordinate the request. The Data Protection Officer will provide advice and oversight where required.

Individual Rights

10.2 Individuals have rights over their personal data. These include:

- the right to be informed about how their personal data is collected and used
- the right of access to their personal data
- the right to have inaccurate personal data corrected and incomplete personal data completed
- the right to have personal data erased in specified circumstances
- the right to restrict processing in specified circumstances
- the right to receive and transfer personal data in a structured, commonly used and machine-readable format where the right to data portability applies
- the right to object to processing in specified circumstances
- rights relating to automated decision-making and profiling
- the right to withdraw consent where consent is relied upon

10.3 These rights are not absolute. Their application depends on the circumstances, the purpose of the processing, the lawful basis relied upon and any relevant legal exemptions.

10.4 Rights relating to automated decision-making and profiling are addressed in Section 13. Data protection complaints are addressed in Section 17.

Making an Information Rights Request

10.5 An individual or their authorised representative may submit an information rights request verbally or in writing. A request does not need to refer to the UK GDPR, use the term "subject access request" or follow a prescribed format.

10.6 Any member of staff who receives or identifies an information rights request must forward it immediately to the relevant academy Data Protection Lead. Staff must not delay the request by asking the individual to complete a form or submit it to another address.

10.7 The Data Protection Lead will record and manage the request, coordinate the required searches and issue the response in accordance with the Trust's procedures.

10.8 The Data Protection Officer will provide advice on complex requests, exemptions, refusals and other matters requiring specialist advice.

10.9 Operational arrangements for handling Subject Access Requests are set out in the Trust's Subject Access Request Procedure.

10.10 The Trust will only request proof of identity where it has reasonable doubts about the requester's identity. Any information requested for verification will be proportionate to the nature and sensitivity of the personal data involved.

10.11 Where a request is made by a representative, the Trust will obtain evidence of their authority to act on behalf of the individual. Further requirements relating to requests made on behalf of children are set out in Section 11.

Subject Access Requests

10.12 A subject access request gives an individual the right to receive:

- confirmation of whether the Trust is processing their personal data
- a copy of their personal data
- the supplementary information required by Data Protection Legislation

10.13 The right of access relates to the individual's personal data rather than an automatic right to receive complete documents. Where appropriate, the Trust will provide the relevant personal data through extracts, summaries or redacted copies.

10.14 Any such response must provide a complete and intelligible copy of the personal data falling within the scope of the request.

10.15 The Trust will undertake searches which are reasonable and proportionate in the circumstances. Searches will cover the systems, records, locations and individuals reasonably likely to hold relevant personal data.

10.16 The Data Protection Lead will coordinate searches with relevant staff, the ICT Team, central service leads and processors. All staff must cooperate promptly and preserve information which falls within the scope of the request.

Time Limits

10.17 The Trust will respond to a subject access request without undue delay and normally within one calendar month of receipt.

10.18 Where proportionate identity verification is required, the response period will begin when the Trust receives the information needed to confirm the requester's identity.

10.19 Where the Trust reasonably requires clarification to identify the information or processing activities covered by the request, it will seek clarification promptly. The response period will pause while the Trust awaits the clarification and resume when the required information is received.

10.20 The Trust will not seek clarification solely to delay responding or require the requester to narrow a request which is already sufficiently clear.

10.21 Where a request is complex or the individual has made a number of requests, the Trust may extend the response period by up to two further calendar months. The Trust will inform the requester of the extension and the reasons for it within the initial one-month period.

10.22 School holidays, closure periods and staff absence do not suspend or extend the statutory response period.

Reviewing and Disclosing Information

10.23 Before disclosure, the Trust will review the information to:

- confirm that it is the requester's personal data
- remove information outside the scope of the request
- identify personal data relating to other individuals
- consider whether any legal exemption applies

- apply appropriate and effective redactions
- ensure that the response is intelligible and secure

10.24 The Trust will not disclose personal data relating to another individual unless:

- the other individual has consented to the disclosure
- it is reasonable to disclose the information without their consent
- another legal provision requires or permits the disclosure

10.25 When deciding whether it is reasonable to disclose another individual's personal data without their consent, the Trust will consider:

- the nature of the information
- any duty of confidentiality owed to the other individual
- any steps taken to seek their consent
- whether the other individual is able to give consent
- any express refusal of consent

10.26 Legal exemptions will be considered individually and applied only to the information covered by the exemption. The reasons for applying an exemption will be documented. The Data Protection Lead will seek advice from the Data Protection Officer where an exemption, refusal or significant redaction is being considered.

10.27 Information will normally be provided electronically where the request was made electronically, unless the requester asks for another format. The Trust will use a secure and accessible method which reflects the nature and sensitivity of the information.

Fees and Refusing Requests

10.28 The Trust will normally respond to information rights requests free of charge.

10.29 Where a request is manifestly unfounded or excessive, taking account of whether it is repetitive, the Trust will either:

- charge a reasonable fee based on the administrative cost of responding
- refuse to act on the request

10.30 The Trust may charge a reasonable fee for further copies of personal data already provided where permitted by law.

10.31 The Trust bears responsibility for demonstrating why a request is manifestly unfounded or excessive. The Data Protection Officer must be consulted before a fee is charged or a request is refused.

10.32 Where the Trust refuses to act on a request, it will inform the requester without undue delay and within one calendar month. The response will explain:

- the reasons for the refusal
- the right to make a data protection complaint to the Trust
- the right to complain to the Information Commissioner's Office
- the right to seek a judicial remedy

Other Information Rights Requests

10.33 Requests for rectification, erasure, restriction, portability or objection will be recorded and handled through the same internal referral process.

- 10.34** The Trust will respond without undue delay and within the applicable statutory period. Where the Trust does not uphold a request, it will explain its decision and the individual's complaint and appeal rights.
- 10.35** Where personal data has been rectified, erased or restricted, the Trust will inform relevant recipients where required by law.

11. Children's Information and Parental Requests

Protecting Children's Information

- 11.1** Children require specific protection because they are often less aware of the risks, consequences and rights associated with the processing of their personal data.
- 11.2** When processing children's personal data, the Trust will:
- place the child's best interests at the centre of its decision-making
 - use personal data in ways the child would reasonably expect
 - apply appropriate safeguards reflecting the child's age and level of understanding
 - limit collection and use to what is necessary
 - explain the processing in clear and age-appropriate language
 - support children to understand and exercise their information rights
- 11.3** Children have the same information rights as adults. These rights belong to the child, even where a parent, carer or other representative exercises them on the child's behalf.
- 11.4** The Trust will provide age-appropriate privacy information for pupils. Where appropriate, different versions will be provided for younger pupils, older pupils and parents or carers.

Children's Consent

- 11.5** The Trust will not assume that consent is required solely because the processing relates to a child. The most appropriate lawful basis will be identified in accordance with Section Seven.
- 11.6** Where the Trust relies on a child's consent outside the provision of an online information society service, it will assess whether the child has sufficient understanding to provide informed consent. There is no fixed age for this assessment.
- 11.7** Where an online information society service is offered directly to a child and consent is relied upon:
- a child aged 13 or over is entitled to provide their own consent
 - for a child under 13, consent must be authorised by a person with parental responsibility
- 11.8** The Trust will make reasonable efforts to verify parental responsibility where parental authorisation is required.

Parental Requests

- 11.9** Parents and carers do not have an automatic right under Data Protection Legislation to access their child's personal data. Parental responsibility alone does not transfer the child's information rights to the parent.
- 11.10** The Trust will accept a parent or other representative exercising a child's information rights where:
- the child has authorised the person to act on their behalf
 - the child does not have sufficient understanding to exercise the right independently
 - allowing the person to act is clearly in the child's best interests
- 11.11** Where a child has sufficient understanding, the Trust will normally respond directly to the child. A parent or other representative will only act on the child's behalf where the child has authorised this or where it is clearly in the child's best interests.

11.12 When assessing whether a child has sufficient understanding, the Trust will consider:

- child's age, maturity and stage of development
- their ability to understand the nature of the request
- their ability to understand the information and any consequences of disclosure
- the nature and sensitivity of the personal data
- the child's views
- any relevant communication needs

11.13 Before disclosing personal data to a parent, carer or representative, the Trust will consider:

- whether the person has parental responsibility or other authority to act
- any court orders or restrictions relating to parental responsibility or contact
- the child's competence and views
- whether the child provided the information in confidence
- any duty of confidentiality owed to the child
- any safeguarding concerns or allegations involving the requester
- the possible consequences of disclosure or non-disclosure
- whether disclosure is in the child's best interests

11.14 The Trust will verify parental responsibility or authority where this is unclear or where the nature of the information requires further assurance.

Routine Information Sharing with Parents

11.15 Nothing in this section prevents academies from sharing routine information with parents or carers about a pupil's education, attendance, behaviour, progress, welfare or safety where the sharing is lawful and appropriate.

11.16 A request for copies of a child's personal data or to exercise another information right must be referred to the academy Data Protection Lead and handled under Sections 10 and 11.

Educational Records

11.17 The separate parental right of access to educational records under the Education (Pupil Information) (England) Regulations 2005 applies to maintained schools and does not apply to academies.

11.18 Requests from parents or carers for personal data contained within a pupil's educational record will be considered under the child's right of access and handled in accordance with Sections 10 and 11.

Withholding Information

11.19 The Trust will consider all relevant legal exemptions before disclosing a child's personal data. Education information will be withheld to the extent that disclosure is likely to cause serious harm to the physical or mental health of the child or another person.

11.20 Information will also be withheld or redacted where another exemption applies, including where disclosure would:

- reveal protected personal data relating to another individual
- breach a duty of confidence where a relevant statutory exemption or restriction applies and its applicable legal conditions have been met
- disclose legally privileged information

- prejudice specified safeguarding, regulatory or criminal matters
- disclose information protected by court rules or another legal restriction

11.21 Exemptions will be considered individually and applied only to the information they cover. The reasons for withholding information will be documented.

11.22 The academy Data Protection Lead will manage the request and seek advice from the Data Protection Officer where the child's competence, parental authority, best interests, safeguarding risks or application of an exemption requires specialist consideration.

11.23 Any safeguarding concern identified through an information rights request must be referred immediately through the Trust's safeguarding procedures.

12. Biometrics, CCTV, Photographs and Videos

- 12.1** Images, recordings and biometric information which identify an individual are personal data and must be processed in accordance with this policy.
- 12.2** A photograph or video is not biometric data solely because it shows an individual's face or physical characteristics. It becomes biometric data where specific technical processing is used to identify the individual uniquely.

Biometric Information

- 12.3** No academy will introduce or materially change an automated biometric recognition system without:
- prior approval from the Chief Executive
 - consultation with the Data Protection Officer
 - completion of a Data Protection Impact Assessment
 - identification of an Article 6 lawful basis and an Article 9 condition
 - confirmation that the processing is necessary and proportionate
 - appropriate consultation and privacy information
 - suitable contractual and security arrangements
- 12.4** Before processing the biometric information of a pupil under 18 through an automated biometric recognition system, the academy will:
- notify each parent or person with parental responsibility whom it is required to notify
 - explain the nature, purpose and operation of the system
 - explain the pupil's and parents' rights to object
 - obtain written consent from at least one parent or person with parental responsibility
- 12.5** The academy will not process the pupil's biometric information where:
- pupil objects or refuses to participate
 - written consent has not been obtained from at least one parent or person with parental responsibility
 - a parent or person with parental responsibility objects in writing
 - consent has been withdrawn
- 12.6** A pupil's objection does not need to be made in writing and overrides any parental consent. Pupils will receive information about their right to object in a form appropriate to their age and understanding.
- 12.7** Where biometric information is not processed, the academy will provide a reasonable alternative which does not disadvantage the pupil or place an additional burden on the pupil or their parents.
- 12.8** When a pupil reaches the age of 18, the academy will review the lawful basis for continued processing. Parental consent will no longer apply.
- 12.9** Biometric information will:
- only be used for the purpose for which it was collected
 - be subject to strict access controls
 - be stored securely
 - not be disclosed except where lawful and necessary

- be deleted when it is no longer required
- be deleted where consent is withdrawn or the pupil objects
- be deleted when the pupil leaves the academy unless a lawful and documented reason requires continued retention

12.10 The Trust will not use live facial recognition technology within its academies.

Adult Biometric Information

12.11 Where the Trust processes biometric information relating to a member of staff or another adult, it will identify and document an Article 6 lawful basis and an Article 9 condition and provide appropriate privacy information. Where consent is relied upon, it must meet the requirements in Section Seven and the individual must have a genuine choice.

12.12 The Trust will provide an alternative arrangement where appropriate.

CCTV and Video Surveillance

12.13 The Trust uses CCTV and other video surveillance systems for specified purposes such as protecting pupils, staff, visitors and property, supporting site security and preventing or investigating incidents.

12.14 CCTV and surveillance systems will be operated in accordance with the Trust's separate CCTV Policy. The Trust will ensure that:

- each system has a documented purpose and lawful basis
- surveillance is necessary and proportionate
- a Data Protection Impact Assessment is completed where required
- cameras are positioned to avoid unnecessary recording
- clear signs inform individuals that surveillance is taking place
- access to recordings is restricted to authorised individuals
- recordings are retained for no longer than required
- disclosures are lawful, necessary and recorded
- systems receive regular reviews

12.15 Audio recording, covert surveillance and recording in areas where individuals have a heightened expectation of privacy will not take place unless exceptional circumstances make it lawful, necessary and proportionate. Such processing requires prior senior authorisation and consultation with the Data Protection Officer.

12.16 Requests for CCTV footage, including requests from individuals, the police, insurers or other organisations, will be handled under the CCTV Policy and the relevant provisions of this policy.

Photographs and Videos

12.17 The Trust takes and uses photographs and videos for purposes including:

- teaching and learning
- recording pupil work and achievement
- identification and administration
- safeguarding and security
- staff training and professional development
- communicating with pupils, parents and the Trust community
- celebrating Trust and academy activities

- publicity, publications, websites and social media

12.18 The Trust will identify an appropriate lawful basis before taking or using photographs and videos. Consent is not required where another lawful basis applies.

12.19 The Trust will normally seek consent for optional publicity uses, including publication on public websites, social media and external promotional materials. Where consent is relied upon:

- the intended uses will be explained clearly
- consent choices will be specific
- a record of consent will be maintained
- refusal will not disadvantage the individual
- consent will be reviewed where appropriate
- withdrawal will apply to future use

12.20 Where consent is withdrawn, the Trust will take reasonable steps to stop further use and remove online material under its control. Withdrawal does not require the recall of printed materials already distributed or copies outside the Trust's control.

12.21 The Trust will avoid publishing a pupil's full name alongside their photograph unless this is necessary, lawful and appropriately authorised.

12.22 Staff must only take, store or share photographs and videos using approved equipment, accounts, systems and platforms. Personal devices and personal accounts must not be used.

12.23 Photographs and videos must not be taken in toilets, changing facilities or other areas where individuals have a heightened expectation of privacy, except where an exceptional safeguarding or legal reason has been authorised.

Photography and Recording at Events

12.24 Each academy will determine whether parents, carers and visitors are permitted to take photographs or recordings at events. The academy will communicate any restrictions before or during the event.

12.25 Where personal photography is permitted, parents, carers and visitors must:

- follow academy instructions
- use images only for personal or household purposes
- avoid photographing or recording individuals where the academy has prohibited this
- respect requests relating to safeguarding, privacy and pupil safety

12.26 The Trust is not responsible for photographs or recordings taken independently by parents, carers or visitors for personal or household purposes. The Trust will take reasonable steps to address inappropriate recording during Trust or academy activities.

13. Artificial Intelligence and Automated Decision-Making

Artificial Intelligence

- 13.1** The Trust may use artificial intelligence, including generative artificial intelligence, where its use supports an approved educational or operational purpose and complies with Data Protection Legislation, relevant Department for Education guidance and the Trust's policies and procedures
- 13.2** Staff and other authorised users must only use artificial intelligence systems approved by the Trust. Personal Data must not be entered into publicly available or unapproved artificial intelligence systems
- 13.3** Personal Data may only be processed through an approved artificial intelligence system where:
- there is a documented purpose and lawful basis
 - the use is necessary, fair and proportionate
 - only the minimum Personal Data required is used
 - appropriate privacy information has been provided
 - the system has appropriate security, contractual, retention and international transfer arrangements
 - any required Data Protection Impact Assessment has been completed
 - the use complies with the Trust's safeguarding and information security requirements
- 13.4** Special Category Personal Data, Criminal Conviction Data, safeguarding information and other highly confidential information must not be entered into an artificial intelligence system unless the particular use has been expressly approved and the additional legal and security requirements have been satisfied.
- 13.5** Before procuring, introducing or materially changing an artificial intelligence system which processes Personal Data, the relevant lead must consult the Trust's ICT Team and Data Protection Officer.
- 13.6** The assessment must consider:
- the purpose and necessity of the proposed processing
 - the categories and volume of Personal Data involved
 - whether the supplier will retain or use information to train or improve its models
 - security, access controls, retention and deletion
 - the supplier's status and contractual obligations
 - international transfers
 - risks of inaccurate, biased or discriminatory outputs
 - the effect on children and other vulnerable individuals
 - whether a Data Protection Impact Assessment is required
- 13.7** Artificial intelligence outputs must be checked by a suitably competent member of staff before they are used. Staff remain responsible for the accuracy, appropriateness and lawful use of any information or output produced by an artificial intelligence system
- 13.8** Artificial intelligence output used as part of Trust business may form part of the Trust's records and may be subject to retention, disclosure, information rights and Freedom of Information requirements.

Automated Decision-Making

- 13.9** A decision is based solely on automated processing where there is no meaningful human involvement in taking the decision. A decision is significant where it produces a legal effect or has a similarly significant effect on an individual.
- 13.10** Human involvement must be genuine and carried out by a person with the authority, competence and information necessary to review the automated output, consider other relevant information and change the proposed decision. Merely approving or accepting an automated recommendation will not constitute meaningful human involvement.
- 13.11** The Trust will not use solely automated processing to make a significant decision about an individual unless:
- the processing is permitted by Data Protection Legislation
 - an appropriate lawful basis and any additional condition have been identified
 - the proposed use has been approved by the Chief Executive following consultation with the Data Protection Officer and the Trust's ICT Team
 - a Data Protection Impact Assessment has been completed
 - appropriate safeguards have been implemented
- 13.12** Additional restrictions apply where a significant automated decision involves Special Category Personal Data. Such processing must not take place unless the specific legal conditions for that processing have been satisfied and the Data Protection Officer has been consulted.
- 13.13** The Trust will ensure that decisions concerning matters such as admissions, exclusions, behaviour or disciplinary action, safeguarding, special educational needs and disabilities, employment, performance or access to significant services involve meaningful human consideration.
- 13.14** Where the Trust makes a significant decision based solely on automated processing, it will take appropriate steps to:
- inform the individual that automated processing has been used
 - provide meaningful information about how the decision was reached and its likely consequences
 - enable the individual to make representations about the decision
 - enable the individual to challenge the decision
 - provide meaningful human intervention and reconsideration of the decision
 - correct inaccurate Personal Data and address inappropriate or discriminatory outcomes
- 13.15** The Trust will monitor artificial intelligence and automated processing for accuracy, fairness, security, bias and unintended consequences. Systems will be reviewed when their purpose, operation, supplier, data use or level of risk materially changes.

14. Data Protection by Design, DPIAs and Accountability Records

Data Protection by Design and Default

- 14.1** The Trust will embed data protection into the design and operation of its systems, services, projects, policies and working practices from the outset and throughout their lifecycle.
- 14.2** Before introducing or materially changing a project, system, supplier, service or processing activity involving personal data, the relevant lead must complete an initial data protection screening assessment and involve the Data Protection Officer and ICT Team where appropriate.
- 14.3** The Trust will apply measures which include:
- limiting the personal data collected and access to it
 - applying privacy-protective default settings
 - establishing retention and deletion arrangements
 - using appropriate security measures
 - using anonymisation or pseudonymisation where appropriate
 - providing clear privacy information and supporting information rights
 - reviewing suppliers, contracts and international transfers
 - testing and reviewing controls throughout the processing lifecycle
- 14.4** When designing or operating an online service likely to be accessed by children, the Trust will take account of their age, understanding, needs and the risks arising from the processing.

Data Protection Impact Assessments

- 14.5** A Data Protection Impact Assessment must be completed before processing begins where the proposed processing is likely to result in a high risk to the rights and freedoms of individuals.
- 14.6** High-risk processing may include:
- new technologies, artificial intelligence or significant automated decision-making
 - systematic monitoring, tracking or profiling
 - large-scale processing of Special Category Personal Data or Criminal Conviction Data
 - biometric identification or large-scale CCTV monitoring
 - high-risk processing involving children or other vulnerable individuals
 - matching information from different sources in unexpected ways
 - processing which could prevent access to a service, opportunity or right
- 14.7** The Data Protection Impact Assessment will describe the processing and its purpose, identify the lawful basis, assess necessity and proportionality, record risks and safeguards, include relevant consultation and DPO advice and identify responsibility for agreed actions and residual risks.
- 14.8** The relevant project or service lead owns the Data Protection Impact Assessment and remains responsible for completing agreed actions. The Data Protection Officer provides independent advice and monitors compliance but does not approve the operational decision to proceed.
- 14.9** The appropriate Executive Team member must approve any decision to proceed where material data protection risks remain. Where a high residual risk cannot be reduced, the Trust will consult the Information Commissioner's Office before processing begins.

14.10 The Data Protection Impact Assessment will be reviewed where the nature, purpose, scope, context or risk of the processing changes.

Accountability Records

14.11 The Trust will maintain a Record of Processing Activities covering personal data processed across the Trust and its academies. This will include the purposes and lawful bases for processing, categories of individuals and personal data, recipients and processors, international transfers, retention periods, security measures and links to relevant privacy notices and Data Protection Impact Assessments.

14.12 Executive Team members, central service leads, Headteachers and academy Data Protection Leads must provide the information required to maintain these records and report material changes to processing.

14.13 The Trust will retain appropriate evidence of compliance, including privacy notices, assessments, agreements, consent records, information rights requests, Personal Data Breaches, complaints, training and assurance activity.

14.14 Accountability records will be accurate, current and available for review by the Data Protection Officer, Trust Board and Information Commissioner's Office where required.

15. Security, Retention and Disposal

Information Security

- 15.1** The Trust will implement appropriate technical and organisational measures to protect personal data. These measures will reflect the nature of the information, the purposes of processing, current security risks and the potential effect on individuals.
- 15.2** Security arrangements will protect the confidentiality, integrity, availability and resilience of personal data and support the timely restoration of access following an incident.
- 15.3** Security measures will include, where appropriate:
- role-based access controls and secure authentication
 - encryption and secure methods of transferring information
 - physical security for buildings, equipment and paper records
 - secure configuration of devices, systems and networks
 - backup, recovery and business continuity arrangements
 - protection against malware and unauthorised access
 - system updates, testing, monitoring and access reviews
 - appropriate controls for remote and mobile working
- 15.4** Staff and other authorised users must:
- access personal data only where required for their role
 - use Trust-approved systems, devices and communication methods
 - protect passwords, devices and paper records
 - check recipients and attachments before sending information
 - not use personal accounts, storage or unapproved applications for Trust information
 - report lost devices, misdirected communications, unauthorised access and other security concerns immediately
- 15.5** Access will be removed or amended promptly where an individual changes role, no longer requires access or leaves the Trust. Enhanced controls will apply to Special Category Personal Data, Criminal Conviction Data, safeguarding information and other higher-risk information.
- 15.6** Processors and other organisations handling personal data on the Trust's behalf must meet the requirements set out in Section Nine.

Retention

- 15.7** The Trust will retain personal data only for as long as required for the purpose for which it was collected, including any legal, regulatory, safeguarding, contractual, operational or archival requirement.
- 15.8** Detailed retention periods and responsibilities are set out in the Records Management and Retention Schedules Policy.
- 15.9** Relevant service leads, Headteachers and academy Data Protection Leads must support regular reviews of records within their areas and arrange secure disposal when the applicable retention period expires.
- 15.10** Routine disposal will be suspended where information remains relevant to an information rights request, complaint, employment matter, legal proceeding, investigation, audit, regulatory enquiry, safeguarding concern or another documented requirement.

15.11 Personal data retained beyond its usual retention period must have a recorded reason and review date. Where information remains useful for statistical, research or reporting purposes, the Trust will consider anonymising it instead of retaining identifiable personal data.

15.12 Personal data held within backup systems will remain protected and will be deleted or overwritten in accordance with the Trust's backup and retention arrangements. Restored information remains subject to the applicable retention and disposal requirements.

Disposal

15.13 Personal data must be disposed of securely when it is no longer required. The disposal method will reflect the format and sensitivity of the information.

15.14 Secure disposal will include, where appropriate:

- confidential destruction of paper records
- secure deletion of electronic records
- secure erasure or destruction of storage media
- removal of information from devices before reuse or disposal
- use of approved confidential waste and technology disposal providers

15.15 Third-party disposal providers must be subject to appropriate contractual, security and assurance arrangements. The Trust will maintain records of scheduled or material disposal activity where appropriate.

15.16 Any loss, unauthorised destruction or insecure disposal of personal data must be reported and managed under Section 16.

16. Personal Data Breaches

Reporting a Breach

16.1 All actual or suspected Personal Data Breaches must be reported immediately, regardless of their apparent seriousness or whether all details are known.

16.2 Personal Data Breaches include:

- sending personal data to the wrong recipient
- losing paper records, devices or storage media
- unauthorised access, use, disclosure, alteration or deletion
- losing access to personal data through a cyberattack or system failure
- accessing or disclosing personal data without a work-related reason

16.3 Academy staff must report the matter immediately to the academy Data Protection Lead and the Trust's Data Protection Officer using the Trust's breach-reporting process. Central Trust staff must report it to the Data Protection Officer. Incidents involving systems, devices, accounts or cyber security must also be reported to the ICT Team.

16.4 Staff must not:

- delay reporting while investigating the incident
- contact affected individuals unless instructed to do so
- delete relevant emails, logs, documents or other evidence
- attempt to conceal or resolve the matter without reporting it

Managing a Breach

16.5 The academy Data Protection Lead or relevant central service lead will support immediate containment, preserve relevant evidence and provide the Data Protection Officer with the information required to assess the incident.

16.6 The Data Protection Officer will coordinate the assessment and response on behalf of the Trust. The assessment will consider the nature and sensitivity of the personal data, the individuals affected, existing protections, the likelihood and severity of harm, containment action and any safeguarding, employment, legal or regulatory implications. Responsibility for compliance remains with the Trust as Data Controller.

Reporting to the Information Commissioner's Office

16.7 Where a Personal Data Breach is likely to result in a risk to the rights and freedoms of individuals, the Trust will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

16.8 Internal reporting delays do not extend the statutory period. Where notification takes place after 72 hours, the Trust will record the reasons for the delay. Where full information is unavailable, the Trust will provide available information and submit further information in phases without undue delay.

16.9 The Data Protection Officer will coordinate any regulatory notification and inform the Chief Executive and relevant senior leaders. They will also consider whether notification to another regulator, insurer, law enforcement body or public authority is required.

Informing Affected Individuals

16.10 Where a Personal Data Breach is likely to result in a high risk to an individual's rights and freedoms, the Trust will inform the affected individual without undue delay unless a legal exception applies. The communication will explain the nature and likely consequences of the breach, the action taken or proposed, any steps the individual should take and how to contact the Data Protection Officer.

Breach Records and Review

16.11 The Trust will record every confirmed Personal Data Breach, including breaches which do not require regulatory notification. The record will include the circumstances, personal data and individuals affected, risk assessment, containment action, notification decisions and remedial action.

16.12 Following a breach, the relevant service lead, academy Data Protection Lead, ICT Team and Data Protection Officer will review its cause and ensure agreed actions are completed. The Data Protection Officer will monitor trends and report significant incidents, risks and themes through the Trust's assurance and governance arrangements.

17. Data Protection Complaints

Making a Complaint

- 17.1** Individuals have the right to complain where they consider that the Trust has infringed Data Protection Legislation when processing their personal data or personal data belonging to someone they represent.
- 17.2** Complaints include concerns about the collection, accuracy, security, retention, use or disclosure of personal data, the handling of an information rights request, a Personal Data Breach, the provision of privacy information or another alleged failure to comply with Data Protection Legislation.
- 17.3** Individuals do not need to use legal terminology or complete a particular form. Complaints should be directed to the Data Protection Officer using the contact details in Section Two, although the Trust will accept a complaint received through any appropriate channel.
- 17.4** Staff receiving a data protection complaint must forward it immediately to the Data Protection Officer and, where it relates to an academy, copy it to the relevant Data Protection Lead.

Handling Complaints

- 17.5** The Data Protection Officer will coordinate the handling and investigation of data protection complaints. Where a complaint concerns the conduct or decision of the Data Protection Officer, the Chief Executive will appoint an appropriate senior officer or independent adviser to oversee the matter.
- 17.6** The Trust will acknowledge receipt of a complaint within 30 days. This period begins on the day after the complaint is received. Where the final day falls on a weekend or public holiday, the deadline will be the next working day. School holidays, closures and staff absence do not suspend this period, and appropriate year-round arrangements will be maintained.
- 17.7** The Trust will only request evidence of identity or authority to act for another person where this is reasonable and proportionate. Complaints made by or on behalf of children will be handled in accordance with Section 11.
- 17.8** The Trust will investigate and respond to complaints fairly, proportionately and without undue delay. The investigation will include appropriate enquiries into the circumstances and consideration of whether the Trust has complied with Data Protection Legislation and its own policies and procedures.
- 17.9** The complainant will be kept informed of the progress of the investigation without undue delay, including any revised timescale and the reasons for a delay.
- 17.10** The written outcome will explain the matters investigated, the Trust's findings and reasons, whether the complaint has been upheld in whole or in part, any corrective action to be taken and the complainant's right to raise the matter with the Information Commissioner's Office.
- 17.11** Where a complaint identifies an error, control weakness or failure to comply with Data Protection Legislation, the Trust will take appropriate corrective action and monitor its completion.
- 17.12** Where a complaint also concerns employment, safeguarding, educational provision or another service matter, those elements will be considered under the relevant procedure. This will not unnecessarily delay the investigation of the data protection issues.

Information Commissioner's Office

17.13 Individuals have the right to raise their concerns with the Information Commissioner's Office at any stage and do not have to complete the Trust's complaints process first. The Trust will cooperate with the Information Commissioner's Office and provide information where legally required.

Recording and Monitoring

17.14 The Trust will retain an appropriate record of each complaint, its acknowledgement, the enquiries undertaken, the outcome and any resulting action, in accordance with its Records Management and Retention Schedules Policy.

17.15 The Data Protection Officer will monitor complaint themes, response times and corrective actions and report significant matters to the Trust Board or Audit and Risk Committee as appropriate.

18. Training, Monitoring and Review

Training and Awareness

18.1 All staff, volunteers and other authorised users with access to Personal Data must complete appropriate data protection training.

18.2 Training will include:

- induction training before or shortly after access to Personal Data is granted
- regular refresher training
- updates following material legal, regulatory, policy or procedural changes
- targeted training following incidents, audit findings or identified risks

18.3 Additional role-specific training will be provided to academy Data Protection Leads and staff involved in:

- information rights requests
- safeguarding and pupil support
- admissions and pupil records
- human resources and recruitment
- governance and complaints
- procurement and contract management
- information technology and cyber security
- CCTV, biometrics and artificial intelligence

18.4 Staff must understand:

- their responsibilities under this policy
- how to handle Personal Data securely
- how to recognise and report information rights requests
- how to recognise and report Personal Data Breaches
- when to seek advice from the academy Data Protection Lead or Trust Data Protection Officer

18.5 The Trust will maintain records of training completion and follow up any overdue or incomplete training.

Monitoring and Assurance

18.6 The Data Protection Officer will monitor the Trust's compliance with Data Protection Legislation and this policy.

18.7 Monitoring and assurance activity will include, where appropriate:

- reviewing the Record of Processing Activities
- reviewing Data Protection Impact Assessments
- monitoring information rights requests and response times
- reviewing Personal Data Breaches, complaints and corrective actions
- reviewing privacy notices, consent arrangements and lawful basis records
- checking processor contracts, data sharing arrangements and international transfers
- reviewing retention and disposal arrangements
- monitoring training completion
- undertaking audits, compliance reviews and risk assessments

- following up agreed actions
- 18.8** Headteachers, Executive Team members, central service leads and academy Data Protection Leads must provide the information and assurance required to support monitoring and compliance reviews.
- 18.9** Identified weaknesses, risks or non-compliance will be recorded, assigned to an appropriate owner and monitored until resolved.
- 18.10** The Data Protection Officer will report significant incidents, risks and compliance concerns promptly to the Chief Executive and, where appropriate, the Chair of the Trust Board or Chair of the Audit and Risk Committee.
- 18.11** The Data Protection Officer will provide an annual report directly to the Trust Board covering:
- compliance activity and key risks
 - information rights requests
 - Personal Data Breaches
 - data protection complaints
 - Data Protection Impact Assessments
 - training and awareness
 - audits and completed actions
 - priorities and recommendations for the following year

Policy Review

- 18.12** Endeavour Learning Trust owns this policy. The Chief Executive, Director of People and Data Protection Officer are the Policy Leads. The Data Protection Officer is responsible for coordinating its review and proposing any required amendments.
- 18.13** The policy will be reviewed at least annually, or sooner where required following:
- changes to legislation or regulatory guidance
 - changes to the Trust's structure, systems or processing activities
 - significant incidents or complaints
 - audit findings or identified compliance risks
- 18.14** The Audit and Risk Committee will review the policy and recommend it to the Trust Board for approval in accordance with the Scheme of Delegation.
- 18.15** The Trust Board will approve this policy as the Trust's Data Protection Policy and any material amendments to it. In accordance with the Scheme of Delegation, the Chief Executive will approve the provisions relating to biometric information and information security. The Chief Executive must also approve the introduction or material amendment of biometric systems and associated operational arrangements. No academy can introduce or materially change an automated biometric recognition system without this approval.
- 18.16** Approved changes will be communicated to relevant staff and reflected in associated policies, procedures, privacy notices, training and guidance.
- 18.17** Failure to comply with this policy could result in disciplinary action. Breaches by contractors, processors or other external parties will be addressed under the relevant contractual or legal arrangements.

Document Control

Approved for Operation Within	All Endeavour Learning Trust Organisations		
Status	Statutory		
Owner	Endeavour Learning Trust		
Approver	Full Trust Board		
Policy Lead(s)	Neelam Yousaf, Director of People, and Emma Cockburn-Hyde, Head of Governance, Compliance and Risk (Data Protection Officer)		
Date Effective from	September 2026	Date of Next Review	September 2027
Review Period	Annual	Version	September 2026

