Exceed Learning Partnership
• EVERY CHILD • EVERY CHANCE • EVERY DAY •

Data Protection Policy

Author/Owner (Name and Title)	Andy Hibbitt – Deputy Chief Executive Officer
Version Number	Version 5
Date Approved/Reviewed	July 2026
Date of Next Review	September 2027
Approved By	Audit and Risk Committee
Policy Category (Please indicate in bold)	**1 - Academy to implement without amendment** 2 – Academy specific appendices 3 – Academy personalisation required (highlighted)

CONTENTS

Summary of Changes from Previous Version

Version	Date	Author	Summary of Updates
V4	July 2025	Legal	Updated policy to reflect the Data (Use & Access) Act 2025
v5	July 2026	DPO	Added Generative AI (Gen AI) to the Definitions Section Updated Scope - Point J to reference using personal data or special category data with Gen AI platform Updated Section 13 to reference using personal data or special category data with Gen AI platform

			Updated Section 14 - Expanded breach definition to include AI data leaks Added Academy Trust Handbook to include zero-ransomware payment mandate.

1. Purpose

This policy explains how Exceed Learning Partnership meets its legal duties under the Data Protection Act 2018, the UK GDPR, the Data (Use and Access) Act 2025 and related laws.

Exceed Learning Partnership collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Trust or our academies in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with relevant legislation.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation and shall be reviewed annually.

2. Interpretation

Definitions:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The Data (Use and Access) Act 2025 has relaxed restriction on decisions made solely made by automated means.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Trust Personnel: all employees (including both teaching and non-teaching staff), workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our Trust Personnel and Personal Data used in our business for our own purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data (Use and Access) Act 2025: an act that amends, but does not replace, the UK General Data Protection Regulation, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the UK GDPR.

Generative AI (Gen AI): Artificial intelligence tools and applications (including, but not limited to, large language models, image generators, and automated content creation software) capable of generating text, images, code, or audio based on user prompts. Processing Personal Data using unapproved Gen AI platforms—where input data may be retained, re-purposed, or used to train public models without appropriate contractual safeguards—constitutes unauthorised processing under this policy.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Guidelines: The Trust privacy and UK GDPR-related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies, available from the DPO.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Trust collects information about them. These notices may take the form of:

general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or

stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: The Trust's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data, available from the DPO.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

The Trust: Exceed Learning Partnership which is an exempt charity regulated by the Secretary of State for Education. It is a company limited by guarantee registered in England and Wales (Company Number 10660150), whose registered office is 6-9 Railway Court, Ten Pound Walk, Doncaster, DN4 5FB.

3. Introduction

This Data Protection Policy sets out how the Trust ("we", "our", "us", "", “the Trust”) handles the Personal Data of our students, parents, suppliers, employees, workers and other third parties.

This Data Protection Policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.

This Data Protection Policy applies to all Trust Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you for the Trust to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all those Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

Where you have a specific responsibility in connection with Processing, such as capturing Consent, reporting a Personal Data Breach or conducting a DPIA as referenced in this Data Protection Policy or otherwise, then you must comply with the Related Policies and Privacy Guidelines.

This policy is an internal compliance document and not intended for external distribution unless required by regulatory inspection or upon formal request

4. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Trust is exposed to potential fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR. (This is a maximum theoretical threshold, depending on scale and severity)

All Academy Principals, central team departments and Schools are responsible for ensuring all Trust Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

The DPO and Deputy CEO (DCEO) are responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines. The post of DPO is held by Wayne Kilner and they can be reached at 01709 805175 and *dpo@exceedlearningpartnership.com*

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

a. if you are unsure of the lawful basis on which you are relying to process Personal Data (including the legitimate interests used by the Trust) (see 4);

b. if you need to rely on Consent or need to capture Explicit Consent (see 6);

c. if you need to draft Privacy Notices (see 7);

d. if you are unsure about the retention period for the Personal Data being Processed (see 8);

e. if you are unsure what security or other measures you need to implement to protect Personal Data (see 012);

f. if there has been a Personal Data Breach (13);

g. if you are unsure on what basis to transfer Personal Data outside the UK (see paragraph 19);

h. if you need any assistance dealing with any rights invoked by a Data Subject (see 14);

i. whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see 18) or plan to use Personal Data for purposes other than for which it was collected;

j. if you plan to undertake any activities involving Automated Processing including profiling, Automated Decision-Making, or entering any Personal Data or Special Categories of Personal Data into a Generative AI tool or platform (discuss this with the DPO)

k. if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 19); or

l. if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see 20).

5. Personal Data Protection Principles

We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

- processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
- collected only for specified, explicit and legitimate purposes (purpose limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);
- accurate and where necessary kept up to date (accuracy);
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);
- not transferred to another country without appropriate safeguards in place (transfer limitation); and
- made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

6. Lawfulness, fairness and transparency

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The UK GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given their Consent; Where Special Category Data is processed, an additional lawful condition under Article 9 UK GDPR must also apply;
- the Processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests;
- to perform a task in the public interest or as part of an official function and that function has a clear basis in law; or
- to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

More information on the types of data we process and the purposes under the UK GDPR that we rely on, can be found in the relevant Privacy Notices for pupils and employees: Website: https://exceedlp.org.uk/policies-and-procedures/

7. Consent

A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Consent must not be relied upon where there is a clear imbalance of power (e.g. staff-pupil relationships), except where no other lawful basis applies

When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines, so that the Trust can demonstrate compliance with Consent requirements.

8. Transparency (notifying Data Subjects)

The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice in accordance with our Related Policies and Privacy Guidelines.

Links to our Privacy Notices can be found here: *www.exceedlearningpartnership.co.uk/policies-and-procedures/*

9. Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes. Personal data must only be used for the specific purpose it was originally collected for. If the school wishes to use the data for a new or different purpose, this is only permitted where:

- The new purpose is compatible with the original one, as outlined in Article 8A of the UK GDPR; or
- The individual has been informed of the new purpose and, where required, has given their consent.

In all cases, the school must ensure that any further use of personal data remains fair, lawful, and transparent, and that individuals are given a clear opportunity to object where appropriate.

10. Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Trust's data retention guidelines.

11. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

12. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

The Trust maintains a Data Retention Policy and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time. You must comply with the Trust's Data Retention Policy. A copy of this can be requested from the DPO or the DCEO.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Trust's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

You will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

13. Security Integrity and Confidentiality

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must

implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our ICT systems and cyber security and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

Any third-party processor must notify the Trust of any actual or suspected breach without undue delay, as contractually required.

Trust Personnel must not paste, upload, or prompt any Personal Data, Special Categories of Personal Data, or confidential Trust files into public or unvetted Generative AI tools. Personal Data may only be processed using Trust-approved, enterprise-grade AI platforms where a formal contract or Data Processing Agreement (DPA) is in place ensuring that Trust data remains strictly confidential, secure, and is excluded from model training datasets.

14. Reporting a Personal Data Breach

The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commission and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify the Data Subject or any applicable regulator where we are legally required to do so.

The Data Protection Officer will assess whether the breach requires reporting to the ICO within 72 hours in line with regulatory obligations.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO and your Line Manager. You should preserve all evidence relating to the potential Personal Data Breach.

A Personal Data Breach includes, but is not limited to, the inadvertent or deliberate exposure of Personal Data to third-party Generative AI tools or unauthorised cloud databases.

In the event of a critical cyber-incident or ransomware attack compromising Trust data systems, the Trust strictly complies with Department for Education (DfE) guidance and the Academy Trust Handbook requirement prohibiting the payment of cyber-ransom demands under any circumstances.

15. Data Subject's Rights and Requests

A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:

a) withdraw Consent to Processing at any time;

b) receive certain information about the Controller's Processing activities;

c) request access to their Personal Data that we hold;

d) prevent our use of their Personal Data for direct marketing purposes;

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

f) restrict Processing in specific circumstances;

g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

i) object to decisions based solely on Automated Processing, including profiling (ADM);

j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

l) make a complaint to the supervisory authority; and

m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject Access Request you receive to the HR Department or the DPO.

16. Accountability

The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Trust must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines or Privacy Notices;

d) regularly training Trust Personnel on the UK GDPR, DUAA 2025, this Data Protection Policy, Related Policies and Privacy Guidelines, and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Trust must maintain a record of training attendance by Trust Personnel; and

e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. Record-keeping

The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum:

- the name and contact details of the Controller and the DPO; and
- clear descriptions of:
- the Personal Data types;
- the Data Subject types;
- the Processing activities;
- the Processing purposes;
- the third-party recipients of the Personal Data;
- the Personal Data storage locations;
- the Personal Data transfers;
- the Personal Data's retention period; and
- the security measures in place.

18. Training and Audit

We are required to ensure all Trust Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy-related training and ensure your team undergoes similar mandatory training. Training attendance and completion rates will be monitored by the Data Protection Officer or delegated lead to ensure full coverage and remedial training where required."

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

19. Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

The Controller must also conduct a DPIA in respect to high-risk Processing. If you think that a DPIA might be necessary for any Processing, or have any queries about a DPIA, please contact the DPO.

A DPIA must include:

- A description of the Processing, its purposes and the Controller's legitimate interests if appropriate.
- An assessment of the necessity and proportionality of the Processing in relation to its purpose.
- An assessment of the risk to individuals.
- The risk mitigation measures in place and demonstration of compliance.

20. Direct Marketing

We are subject to specific rules and privacy laws when communicating with individuals for non-operational purposes.

For example, prior consent is required for sending electronic communications that could be considered promotional or non-essential (such as emails, texts, or automated calls not directly related to a pupil's education or welfare).

While there is a limited exception known as the "soft opt-in" for organisations that have obtained contact details in the course of providing a service, this typically applies in commercial contexts and is unlikely to be relevant to schools.

As the 'soft opt-in' exemption does not apply to most school-based communications and must not be relied upon without prior approval from the Trust Data Protection Officer.

Individuals must be clearly informed of their right to object to such communications, and any objection must be respected promptly. If someone opts out, their contact details should be retained only to the extent necessary to ensure their preferences are honoured in the future.

21. Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our Trust, or a third party if the recipient has a job-related need to know the information and appropriate arrangements have been put in place. Please contact the DPO for more information.

The following list includes some of the most common reasons for the most usual reasons that the Trust will authorise the disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee, volunteer or student;
- For the prevention or detection of crime;
- For the assessment of any tax or duty;
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract);
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- For the purpose of obtaining legal advice;
- For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of academy trips; To provide information to another educational establishment to which a pupil is transferring;
- To provide information to the Examination Authority as part of the examination process; and to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

The Trust may receive requests from third parties (i.e., those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Trust.

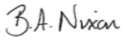
All requests for the disclosure of personal data must be sent to the DPO, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

22. Changes to this Data Protection Policy

We keep this Data Protection Policy under regular review. This version was last updated in July 2025

Policy Reviewed: July 2026

Next Review – September 2027

CEO Signature: 

Chair of Directors Signature: