

DATA PROTECTION AND PRIVACY POLICY

Revised 1 October 2026

Education Appeals

1. INTRODUCTION

EducationAppeals (hereinafter referred to as "The Company") is committed to protecting the privacy, confidentiality and security of personal information entrusted to it by customers, employees, prospective employees, schools, parents, suppliers, contractors, business partners and other individuals.

The Company recognises its responsibilities under applicable UK 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 Regulations 2003 (PECR), where applicable.
- Any other applicable data protection and privacy legislation.

The Company is committed to ensuring that personal information is collected, processed, stored, shared and disposed of lawfully, fairly, transparently and securely.

This policy establishes the principles, responsibilities and procedures that govern how the Company manages personal information and protects the privacy rights of individuals.

2. PURPOSE OF THIS POLICY

The purpose of this policy is to:

- Ensure compliance with applicable UK data protection legislation.
- Protect the personal information of individuals.
- Establish clear rules governing the collection, use, storage and disclosure of personal data.
- Prevent unauthorised access, disclosure, alteration, loss or destruction of personal information.
- Ensure that individuals understand their rights concerning their personal information.
- Establish accountability for data protection throughout the Company.
- Promote a culture of confidentiality, privacy and information security.

3. SCOPE

This policy applies to:

- All employees, directors and officers of the Company.
- Temporary workers, agency staff and interns.
- Contractors, consultants and other individuals working on behalf of the Company.
- Third-party service providers who process personal information on behalf of the Company.

It applies to all personal information processed by the Company, whether held electronically, in paper records, on computer systems, mobile devices, cloud platforms, email systems or any other storage medium.

The policy covers personal information relating to:

- Customers and prospective customers.
- Employees and former employees.

- Schools.
- Parents and appellants.
- Job applicants and prospective employees.
- Suppliers and contractors.
- Business partners and professional contacts.
- Website users and individuals contacting the Company.
- Any other identifiable individual whose information is processed by the Company.

4. DEFINITIONS

For the purposes of this policy:

Personal Data: Any information relating to an identified or identifiable living individual.

Data Subject: The individual to whom personal data relates.

Data Controller: The organisation that determines the purposes and means of processing personal data.

Data Processor: An organisation or individual that processes personal data on behalf of a data controller.

Processing: Any operation performed on personal data, including collection, recording, storage, use, disclosure, alteration, retrieval or deletion.

Special Category Data: Personal data requiring additional protection under UK GDPR, including information concerning health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, sex life or sexual orientation.

Personal Data Breach: A security incident resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. DATA PROTECTION PRINCIPLES

The Company shall comply with the following data protection principles.

5.1 Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and transparently.

Individuals shall be informed about how their personal information is collected, used, stored and shared.

5.2 Purpose Limitation

Personal information shall only be collected for specified, explicit and legitimate purposes.

The Company shall not use personal information for unrelated purposes unless such further processing is legally permitted.

5.3 Data Minimisation

The Company shall only collect personal information that is adequate, relevant and necessary for the purposes for which it is processed.

Unnecessary personal information shall not be collected or retained.

The Company will retain all information for an admission appeal hearing for a period of two years and five years for an exclusion appeal.

5.4 Accuracy

The Company shall take reasonable steps to ensure that personal information is accurate and kept up to date.

Inaccurate information shall be corrected or deleted without unnecessary delay.

5.5 Storage Limitation

Personal information shall not be retained for longer than is necessary for the purposes for which it was collected, subject to applicable legal and regulatory retention requirements.

5.6 Integrity and Confidentiality

The Company shall implement appropriate technical and organisational measures to protect personal information against:

- Unauthorised access.
- Accidental loss or destruction.
- Unlawful processing.
- Unauthorised disclosure.
- Damage or alteration.

5.7 Accountability

The Company shall be responsible for demonstrating compliance with applicable data protection legislation.

Appropriate policies, procedures, records and controls shall be maintained to demonstrate compliance.

6. COLLECTION OF PERSONAL INFORMATION

The Company may collect personal information through various means, including:

- Direct communication with customers, employees and suppliers.
- Website enquiries, online conversations with a virtual assistant and online forms.
- Telephone calls and email correspondence.
- Employment applications and recruitment processes.
- Contracts and commercial transactions.

- Business relationships and professional introductions.
- Third-party service providers and publicly available sources, where legally permitted.

The types of personal information collected may include:

- Names and contact details.
- Postal and email addresses.
- Telephone numbers.
- Employment and professional information.
- Financial and payment information.
- Contractual and transaction information.
- Identification and verification information.
- Website usage and technical information.
- Relevant information regarding Admission and Exclusion Appeals.
- Other information necessary for legitimate business operations.

The Company shall ensure that individuals are informed about the collection and use of their personal information in accordance with applicable legal requirements.

7. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

The Company shall only process personal data where a valid lawful basis exists under Article 6 of the UK GDPR.

Depending on the circumstances, the Company may rely on the following lawful bases:

Consent: Where an individual has freely given clear and informed consent to the processing of their personal information for a specific purpose.

Contractual Necessity: Where processing is necessary to enter into or perform a contract with an individual.

Legal Obligation: Where processing is necessary to comply with a legal or regulatory obligation.

Legitimate Interests: Where processing is necessary for the legitimate interests of the Company or a third party, provided those interests do not override the rights and freedoms of the individual.

Vital Interests: Where processing is necessary to protect someone's life or other vital interests.

Public Task: Where processing is necessary for the performance of a task carried out in the public interest or under official authority, where applicable.

Where special category personal data is processed, the Company shall also identify and satisfy an applicable condition under Article 9 of the UK GDPR and any relevant additional requirements.

The Company shall document the lawful basis relied upon for its processing activities.

8. USE OF PERSONAL INFORMATION

Personal information may be processed for the following business purposes:

- Providing products and services to customers.
- Conducting Admission and Exclusion Appeals.
- Managing customer relationships and enquiries.
- Processing orders, payments and invoices.
- Managing supplier and contractor relationships.
- Recruitment and employment administration.
- Payroll and employee benefits administration.
- Meeting legal, regulatory and contractual obligations.
- Maintaining business and financial records.
- Protecting the Company's property, systems and business interests.
- Preventing fraud and maintaining information security.
- Responding to complaints, disputes and legal claims.
- Conducting legitimate business administration and operations.
- Communicating with individuals about relevant business matters.

Personal information shall only be used for purposes that are lawful and compatible with the purposes originally communicated to individuals.

9 DISCLOSURE AND SHARING OF PERSONAL INFORMATION.

The Company shall not sell personal information to third parties.

Personal information may be shared where necessary and lawful with:

- Professional advisers, including solicitors, accountants and auditors.
- IT service providers and cloud storage providers.
- Payroll and human resources service providers.
- Banks and payment processing providers.
- Insurance providers.
- Regulatory authorities and government bodies.
- Law enforcement agencies, where legally required or permitted.
- Other service providers acting on behalf of the Company.
- Business partners or other organisations where disclosure is lawful and necessary.

The Company shall take reasonable steps to ensure that third parties receiving personal information maintain appropriate confidentiality and security standards.

Where a third party processes personal data on behalf of the Company, an appropriate written data processing agreement shall be put in place where required by law.

10. INTERNATIONAL DATA TRANSFERS

The Company shall not transfer personal information outside the United Kingdom unless the transfer complies with applicable data protection legislation.

Where international transfers are necessary, the Company shall ensure that an appropriate legal transfer mechanism is in place.

This may include:

- An applicable UK adequacy regulation.
- The UK International Data Transfer Agreement (IDTA).
- The UK Addendum to the EU Standard Contractual Clauses.
- Another legally recognised transfer mechanism or exception.

Where necessary, the Company shall undertake appropriate transfer risk assessments and implement supplementary safeguards.

11. DATA SECURITY

The Company shall implement appropriate technical and organisational security measures to protect personal information.

Such measures may include:

- Password protection and access controls.
- Encryption of sensitive information where appropriate.
- Secure electronic storage and backup procedures.
- Antivirus and endpoint protection.
- Network and system security controls.
- Restricted access to confidential information.
- Physical security measures for offices and storage facilities.
- Staff training and confidentiality obligations.
- Secure disposal of paper and electronic records.
- Regular reviews of information security arrangements.

Access to personal information shall be restricted to individuals who require it for legitimate business purposes.

All employees and contractors must maintain the confidentiality and security of personal information.

12. DATA RETENTION AND DISPOSAL

The Company shall retain personal information only for as long as necessary to fulfil the purpose for which it was collected or to meet applicable legal, regulatory, contractual or business requirements.

Retention periods shall be determined according to the nature of the information and the purpose for which it is held.

When personal information is no longer required, it shall be securely deleted, destroyed or anonymised, as appropriate.

The Company shall maintain appropriate data retention and disposal procedures.

13. INDIVIDUAL DATA PROTECTION RIGHTS

Under applicable UK data protection legislation, individuals may have the following rights:

13.1 Right of Access

Individuals may request confirmation as to whether the Company processes their personal information and request access to that information.

13.2 Right to Rectification

Individuals may request that inaccurate or incomplete personal information be corrected.

13.3 Right to Erasure

Individuals may request the deletion of their personal information in certain circumstances.

13.4 Right to Restriction of Processing

Individuals may request that the Company restricts the processing of their personal information in certain circumstances.

13.5 Right to Data Portability

Where applicable, individuals may request a copy of their personal information in a structured, commonly used and machine-readable format.

13.6 Right to Object

Individuals may object to certain types of processing, particularly processing based on legitimate interests and processing for direct marketing purposes.

13.7 Rights Relating to Automated Decision-Making

Individuals have rights and protections in relation to certain solely automated decisions, including profiling, which produce legal or similarly significant effects.

13.8 Right to Withdraw Consent

Where processing is based on consent, individuals may withdraw their consent at any time. Withdrawal shall not affect the lawfulness of processing carried out before consent was withdrawn.

The availability of these rights depends on the circumstances and applicable legal requirements.

14. HANDLING DATA SUBJECT REQUESTS

Individuals wishing to exercise their data protection rights should contact the Company using the contact details provided in this policy.

The Company shall:

- Acknowledge and assess requests appropriately.
- Verify the identity of the requester where reasonably necessary.
- Respond within the applicable statutory timeframe.
- Provide information in a clear and accessible format.
- Explain any lawful reason where a request cannot be fulfilled.
- Maintain appropriate records of requests and responses.

Requests shall generally be dealt with within one month, subject to applicable statutory extensions and exceptions.

The Company shall not *normally* charge a fee for handling a request unless permitted by applicable law if documents are emailed. If documents are required to be printed and posted, there will be a charge.

15. PERSONAL DATA BREACH MANAGEMENT

The Company shall maintain procedures for identifying, reporting, investigating and managing personal data breaches.

A personal data breach may include:

- Loss or theft of a device containing personal information.
- Unauthorised access to company systems.
- Accidental disclosure of personal information.
- Sending confidential information to the wrong recipient.
- Cyberattacks or malicious software incidents.
- Loss, destruction or corruption of personal records.

All employees and contractors must immediately report any suspected or actual personal data breach to the Principal Clerk.

The Company shall investigate the incident and assess the potential risks to affected individuals.

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, the Company shall notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals shall also be informed without undue delay, unless a relevant legal exception applies.

All breaches shall be appropriately documented, including those that do not require notification to the ICO.

16. COOKIES AND WEBSITE PRIVACY

Where the Company operates a website, it shall ensure that cookies and similar technologies are used in accordance with applicable privacy and electronic communications legislation.

The Company shall:

- Explain the use of cookies and similar technologies.
- Obtain consent before placing non-essential cookies where required.
- Provide appropriate cookie management facilities.
- Maintain a separate Cookie Policy where appropriate.
- Protect personal information collected through website forms and online services.

17. DIRECT MARKETING AND COMMUNICATIONS

The Company shall ensure that direct marketing activities comply with applicable data protection and electronic communications legislation.

Marketing communications shall only be sent where an appropriate lawful basis and any required consent or other PECR permission exists.

Individuals shall be provided with a clear and straightforward method of opting out of marketing communications.

The Company shall respect all valid marketing objections and opt-out requests.

Personal information shall not be used for unsolicited marketing in circumstances prohibited by law.

18. EMPLOYEE RESPONSIBILITIES

All employees, directors and contractors must:

- Read and comply with this policy.
- Maintain the confidentiality of personal information.
- Only access information necessary for their duties.
- Use personal information for authorised business purposes.
- Protect passwords, devices and confidential records.
- Avoid sharing personal information with unauthorised individuals.
- Report suspected data breaches immediately.
- Complete any required data protection training.
- Follow Company procedures for storing, transferring and disposing of information.

Employees must not use personal information for personal purposes or disclose confidential information without proper authorisation.

Failure to comply with this policy may result in disciplinary action or termination of contractual arrangements, as appropriate.

19. DATA PROTECTION TRAINING AND AWARENESS

The Company shall ensure that relevant personnel receive appropriate data protection and information security training.

Training may cover:

- UK GDPR principles and responsibilities.
- Handling confidential information.
- Recognising phishing and cyber threats.
- Secure storage and disposal of personal information.
- Recognising and reporting data breaches.
- Handling data subject access requests.
- Confidentiality and information sharing.

Training shall be reviewed periodically to ensure continued awareness and compliance.

20. DATA PROTECTION IMPACT ASSESSMENTS

Where a proposed processing activity is likely to result in a high risk to individuals' rights and freedoms, the Company shall undertake a Data Protection Impact Assessment (DPIA), where required by law.

A DPIA shall consider:

- The nature and purpose of the processing.
- The type and volume of personal information involved.
- The necessity and proportionality of the processing.
- Potential risks to individuals.
- Measures available to reduce or manage identified risks.

The Company shall consult the ICO where required by applicable legislation.

21. DATA PROTECTION GOVERNANCE AND RESPONSIBILITIES

The Company's senior management shall be responsible for ensuring that appropriate data protection arrangements are implemented and maintained.

The designated person responsible for overseeing data protection compliance shall be:

Name/Position: Stephen Payne, Principal Clerk

Email: clerk@educationappeals.com
Telephone: 020 3151 0400

The designated person shall:

- Oversee the implementation of this policy.
- Monitor compliance with data protection requirements.
- Coordinate responses to data protection requests.
- Assist with data breach investigations.
- Promote data protection awareness.
- Maintain relevant policies, procedures and records.
- Escalate significant data protection concerns to senior management.

Where the Company is legally required to appoint a Data Protection Officer (DPO), the appropriate arrangements shall be made.

22. COMPLAINTS AND CONCERNS

Individuals who have concerns about how the Company processes their personal information should contact the Company using the contact details set out below.

The Company shall investigate complaints fairly and respond appropriately.

Individuals also have the right to raise concerns with the UK Information Commissioner's Office (ICO).

Information Commissioner's Office (ICO)

Website: https://ico.org.uk/

Telephone: 0303 123 1113

Individuals are encouraged to contact the Company first, although they are entitled to complain directly to the ICO.

23. POLICY REVIEW AND MONITORING

This policy shall be reviewed at least annually or sooner where necessary, including following:

- Changes in applicable legislation.
- Significant changes to the Company's business activities.
- Changes in the types of personal information processed.
- Significant data protection incidents.
- Changes to relevant systems, processes or third-party arrangements.
- Recommendations from audits or regulatory guidance.

The Company reserves the right to amend this policy to ensure continued compliance with applicable legal and regulatory requirements.

24. CONTACT DETAILS

For questions, requests or concerns relating to this policy or the processing of personal information, please contact:

EducationAppeals
Sopers House
Cuffley, EN6 4RY
clerk@educationappeals.com
020 3151 0400

www.educationappeals.com

25. APPROVAL AND AUTHORISATION

This policy has been reviewed and approved by the Company's management and shall take effect from the date specified below.

Approved by: Stephen Payne

Position: Principal Clerk, CEO and Director

Signature: 

Date: 1 October 2026

Next Review Date: 1 October 2027