**Privacy Policy of Eduvance Limited**

(Last updated: April 17, 2025)

**1. Introduction**

Eduvance Limited (hereinafter referred to as “the Company”) is an educational organization providing professional training programs in the fields of hospitality, catering, and corporate education. In the course of its activities, the Company collects, processes, stores, and transfers the personal data of clients, students, partners, and employees.

The purpose of this Policy is to establish clear rules for handling personal data in accordance with the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the principles of international data privacy legislation (including the European General Data Protection Regulation, GDPR). Eduvance Limited adheres to high data protection standards and ensures strict compliance with applicable legal requirements. The Policy is written in legal language understandable to the general public and is intended for public access on the Company’s website.

**2. Definitions**

To clarify the content of this Policy, the following key terms are defined:

 • Personal Data: Any information relating to an identified or identifiable natural person (data subject), such as name, date of birth, contact details, payment information.

 • Processing of Personal Data: Any operation performed on personal data, including collection, recording, systematization, storage, modification, transfer, dissemination, or deletion of such data.

 • Data Subject: A natural person whose personal data is processed by the Company.

 • Data Protection Officer (DPO): An officer appointed by the Company responsible for monitoring compliance with legal requirements and this Policy on data protection, as well as for communicating with supervisory authorities and data subjects on related matters.

 • Data Controller: A person or organization that determines the purposes and means of personal data processing. In the context of this Policy, the data controller is Eduvance Limited. (In some jurisdictions, this term is referred to as a “personal data operator.”)

 • Data Processor: A third party or organization that processes personal data on behalf of the controller under contract (e.g., a cloud service provider offering data storage services).

 • Data Breach: Any security violation that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. (Also known as a “personal data security breach.”)

**3. Scope of Application**

This Privacy Policy applies to all personal information processed by Eduvance Limited in the course of its activities. It extends to all company divisions and offices, all employees, as well as any external contractors and partners who process personal data on behalf of the Company under contractual obligations.

The Policy covers all categories of data subjects whose data is collected and used by the Company, including (but not limited to): students and participants of educational programs, individual clients, employees, business partners, suppliers, and visitors to the Company’s website. Particular attention is given to the protection of personal data of minors (children) in accordance with applicable legislation and the provisions of this Policy (see section on children).

This Policy applies to personal data regardless of the method of collection or form of storage—be it electronic systems, paper records, data collected via the website, or mobile applications. The Policy is in effect for all cases of personal data processing by the Company, regardless of the data subject’s country of residence or the location of data processing.

**4. Principles of Data Processing**

Eduvance Limited adheres to the seven core principles of personal data processing as stipulated by the UK GDPR and international standards:

 **1. Lawfulness, Fairness, and Transparency**

Personal data is processed on lawful grounds, fairly, and transparently. We always inform data subjects about what data is being collected and how it will be used.

 **2. Purpose Limitation**

Personal data is collected for specific, pre-defined, and lawful purposes and is not further processed in a manner incompatible with those purposes.

 **3. Data Minimization**

We collect and process only the personal data that is necessary to achieve the stated purposes (the principle of data adequacy).

 **4. Accuracy**

We maintain personal data in a current and accurate state. Inaccurate or incomplete data is corrected or deleted without delay where possible.

 **5. Storage Limitation**

Personal data is not stored longer than necessary for the purposes for which it was collected or as required by law. Once this period expires, we securely delete or anonymize the data.

 **6. Integrity and Confidentiality**

We ensure the appropriate security of personal data using technical and organizational safeguards to prevent unauthorized access, loss, or data leaks.

 **7. Accountability**

The Company is responsible for compliance with the above principles and must be able to demonstrate such compliance. We document processing activities and safeguards, and provide reports to regulators when required.

Next sections:

• 5. Categories of Data Collected

 • 6. Purposes and Legal Basis for Processing

 • 7. Cookies and Analytics

 • 8. Disclosure to Third Parties

 • 9. International Data Transfers

 • 10. Data Retention

 • 11. Data Protection and Security Measures

 • 12. Employee and Partner Responsibilities

 • 13. Data Breach Response

 • 14. Data Subject Rights

 • 15. Children’s Data

 • 16. International Operations and Multilingual Support

 • 17. Contact Information

 • 18. Updates to the Policy

**5. Categories of Data Collected**

Depending on the status of the data subject and the nature of the relationship with the Company, Eduvance Limited may collect various categories of personal information. Below are the main categories of personal data we process:

**5.1. Student and Client Data**

 • Identification Information: Full name, date of birth.

 • Contact Information: Email address, phone number, postal address.

 • Payment Details: Bank account or card details, payment history for educational services.

 • Educational Records: Records of training programs and courses attended, enrollment data, academic performance (if applicable).

 • Certificates and Qualifications: Details of any certificates, diplomas, or qualifications obtained through the Company’s programs.

**5.2. Employee Data**

 • Identification Details: Full name, date of birth, nationality; copies of identity documents (passport or other ID).

 • Employment Information: Resume and employment history, job title, hire date, employment contract details, training records.

 • Financial and Tax Data: Salary details, deductions and taxes, bank information for payroll, information required for tax and accounting reporting.

 • Emergency Contacts: Name and contact details of a person to be contacted in case of emergency (e.g., a family member).

 • Other Work-Related Data: For example, vacation schedule, performance evaluations, disciplinary records (where applicable).

**5.3. Partner and Supplier Data**

 • Contact Details: Name of the partner or supplier organization, name and position of the contact person, business address, phone number, email.

 • Contractual and Financial Information: Details of concluded contracts and agreements, history of business relations, banking information for settlements, information about fulfilled obligations and payments.

 • Other Related Data: Any additional information necessary for interaction with the partner or supplier (e.g., training requirements for partner personnel or other service-related details).

**5.4. Website Visitor Data**

 • Technical Information: Data automatically collected when visiting our website, such as IP address, browser type and version, device type, operating system, geographic location (country or city), information from cookies and other unique identifiers.

 • Activity Data: Information on how visitors interact with our website—visited pages, date and time of visit, duration of session, clicks on page elements, on-site search queries, etc. This data is usually collected through cookies and web analytics tools (see Section 7).

 • Voluntarily Submitted Data: Information provided by users through forms on our website, such as feedback forms, program applications, or newsletter subscriptions, may include name, email, phone number, and the content of the message. We use and store this information to respond to inquiries and maintain communication.

The amount of information collected is always limited to the minimum necessary. If we request personal data that is optional, this will be clearly marked (e.g., with the label “optional”). You have the right to refuse to provide non-mandatory information.

**6. Purposes and Legal Basis for Processing**

We process personal data only when there is a lawful basis to do so, as provided by applicable legislation (including UK GDPR and the Data Protection Act 2018). Depending on the circumstances, such legal bases may include:

**Consent**

In certain cases, we request your explicit consent to use your personal data for specific purposes. For example, consent is required for sending you marketing and newsletter emails, using non-essential cookies (analytical or marketing) on our website, or processing special categories of personal data (if such data is ever requested).

You may withdraw your consent at any time by contacting us or using the opt-out tools provided (see also the section on data subject rights). Withdrawal of consent will not affect the lawfulness of processing carried out before the withdrawal.

**Performance of a Contract**

Processing of personal data may be necessary to enter into or fulfill a contract to which you are a party. For instance, we process student and client data to provide educational services, conduct training, and issue certificates (i.e., to fulfill an education contract). Similarly, employee data is processed to perform employment contracts (e.g., payroll, benefits), and partner or supplier data is used to fulfill cooperation or service agreements. Without such data, we would not be able to properly fulfill our contractual obligations.

**Compliance with a Legal Obligation**

In some cases, we are legally required to process personal data to meet statutory obligations. For example, the law may require us to retain certain documents containing personal data for a specified period (e.g., accounting and tax records, employee information for immigration or social insurance authorities). Additionally, if required by court order or law enforcement, we may be obligated to disclose certain information. In such cases, the legal basis for processing is compliance with a legal obligation.

**Protection of Vital Interests**

In rare cases, we may process personal data if it is necessary to protect the vital interests of you or another individual. For example, in an emergency involving health or safety, processing (including sharing data with medical services) may be required to protect someone’s life.

**Legitimate Interests of the Company**

We may process certain personal data on the basis of Eduvance Limited’s legitimate interests or those of third parties, provided that such interests do not override your fundamental rights and freedoms.

**Examples of processing based on legitimate interest include:**

 • maintaining the security of our IT systems and networks

 • fraud prevention

 • improving the quality of our educational services (based on feedback and performance results)

 • sending informational materials to existing clients about similar services (with an easy opt-out option)

In all such cases, we carefully assess our interests through a balancing test to ensure they do not disproportionately infringe on your rights. You have the right to object to processing based on legitimate interests (see Section 14).

Where necessary, we may rely on a combination of the above legal bases for different aspects of processing the same data. If the purpose of processing changes, we will notify you and, if required, seek additional consent.

**7. Cookies and Analytics**

Our website uses cookies and similar technologies to ensure a convenient user experience and the proper functioning of our services. A cookie is a small text file stored on a user’s device when visiting a website. We use cookies to remember your preferences, improve the website’s functionality, and collect statistics and behavioral data to enhance the quality of our content and services.

**Categories of Cookies Used on Our Site**

 • Essential (Necessary) Cookies:

These cookies are necessary for the technical operation of the site. Without them, certain site features would not function properly (e.g., user login, language preferences). These cookies do not collect personal information for marketing and are set automatically based on our legitimate interest in ensuring the site’s functionality.

 • Analytical and Functional Cookies:

These cookies help us understand how users interact with the site and allow us to remember your preferences to improve usability (e.g., autofilling forms). We use analytics to collect aggregated statistics (e.g., number of visitors, most visited pages, navigation paths). This information is anonymized and used to enhance content and navigation.

We only use these cookies with your consent. Upon your first visit to our website, you will be offered the choice to accept or configure cookie settings. You may change your decision at any time by clearing your browser cookies or adjusting preferences via our interface (if available).

 • Marketing Cookies:

Currently, the Company does not use third-party advertising or targeting cookies. If we ever implement such technologies (e.g., for remarketing purposes), they will only be used with your explicit consent.

**Third-Party Analytics**

We may use third-party analytics services (e.g., Google Analytics or similar tools) to understand our audience and improve our content. These services may set their own third-party cookies (such as Google Analytics cookies) and collect anonymized information about your visit. Such data (e.g., anonymized device identifiers, site actions) is processed exclusively for statistical purposes. We contractually require these providers to use the data only for services provided to us and not to disclose it further.

**Cookie Management**

You are free to configure cookie preferences upon your first site visit and may adjust browser settings at any time to block or delete cookies. Note that disabling all cookies may affect some website features. For more on managing cookies, refer to your browser’s help section.

We respect Do Not Track (DNT) browser settings where applicable and will disable third-party tracking where possible. However, we cannot fully guarantee that third-party analytics providers will honor DNT signals. If you have questions about specific cookies used on our site, please contact us (see Section 17).

**8. Disclosure to Third Parties**

Eduvance Limited does not sell or rent users’ personal data. Access to your personal data is granted only to third parties when necessary for the purposes outlined in this Policy, and only with appropriate legal grounds and safeguards. Below are cases in which data may be shared with third parties:

**Within the Eduvance Group**

If the Company has affiliated entities, branches, or subsidiaries (including outside the United Kingdom), personal data may be transferred within the group for administrative purposes, client relationship management, or service delivery. All internal data transfers follow the same confidentiality and security standards as the parent company. Access is granted only to authorized personnel and only when necessary.

**Service Providers (Data Processors)**

We engage external contractors to perform certain functions on our behalf. These data processors may include:

 • Hosting and cloud storage providers

 • IT service providers

 • Email distribution platforms

 • Payment processing systems

 • Analytics and technical support tools

 • Courier services for delivering documents or certificates

Such third-party organizations receive only the information required to fulfill their tasks (data minimization principle). Each processor is bound by a Data Processing Agreement that obliges them to protect information at a level equal to or higher than our own, and to use the data strictly according to our instructions. They may not use the data for their own purposes.

**Business Partners**

As part of educational programs or joint projects, we may cooperate with external institutions such as universities, industry associations, or commercial partners. In some cases, it may be necessary to share information about students or participants (e.g., for external examination registration or certification validation). Such exchanges occur under a confidentiality agreement and only when the partner has a legal basis for receiving the data. Partners must use the data only for the agreed purpose and maintain the same level of data protection.

**Law Enforcement and Government Agencies**

Eduvance Limited may disclose your personal data to public authorities, regulatory bodies, or other third parties if legally required to do so. For example, we may receive a legally binding request from a court, police, or regulatory authority (such as the Information Commissioner’s Office, ICO) to provide specific data. We fulfill such requests strictly according to legal procedures.

**Additionally, we may disclose information when we believe in good faith that it is necessary to:**

 • protect our rights

 • ensure your safety or that of others

 • investigate fraud

 • comply with government inquiries

In all such cases, we aim to notify data subjects (where permitted by law) and limit disclosure to what is strictly required.

**9. International Data Transfers**

Eduvance Limited transfers personal data internationally only when appropriate safeguards are in place to ensure lawful and secure processing. If we need to send or provide access to personal data outside the United Kingdom, such transfer will comply with the UK GDPR, the Data Protection Act 2018, and applicable international legal standards.

**Transfers to Countries with Adequate Protection**

The United Kingdom recognizes a list of countries as providing adequate data protection (e.g., European Economic Area countries and others officially designated by UK authorities). Transfers to these jurisdictions do not require additional authorization; however, we still formalize confidentiality obligations through contracts.

**Transfers to Non-Adequate Countries**

If data must be transferred to a country not considered to offer adequate protection, we ensure additional safeguards are in place. These include:

 • Standard Contractual Clauses (SCCs) approved by the UK Information Commissioner

 • Data Transfer Agreements with recipients

 • Binding Corporate Rules if the transfer is within a multinational group

We also assess the risks involved and, if necessary, implement supplementary measures such as:

 • end-to-end encryption

 • pseudonymization or anonymization

 • strict access controls on the recipient’s side

**Obligations of Foreign Data Recipients**

Any foreign recipient of personal data must agree contractually to confidentiality and security obligations consistent with this Policy and the law. We remain responsible for your data even after the transfer and monitor whether overseas partners comply with the agreed terms.

**Transparency and Assistance**

If you have questions about international data transfers or would like a copy of relevant safeguards (e.g., Standard Contractual Clauses), you may contact us. We will provide available information within reasonable commercial and security limits.

**10. Data Retention**

We retain personal data only for as long as is necessary to fulfill the purposes for which it was collected, unless a longer retention period is required or permitted by law. Retention periods vary depending on the type of data and the applicable legal and operational obligations:

**Student and Client Data**

Data related to educational services is typically retained for the duration of the training program and a reasonable period thereafter (e.g., for certificate re-issuance or course confirmation). Some records (e.g., contracts and payment documentation) may be kept longer to meet accounting or tax requirements.

**Employee Data**

Personnel records are retained for the period of employment, and after termination, for the duration required by labor and archiving laws (usually several years). Financial data such as payroll and tax information is retained according to tax regulations.

**Partner and Supplier Data**

Data from business partners and service providers is stored for the duration of the contractual relationship and, if necessary, beyond — within the applicable limitation periods and financial record-keeping laws.

**Website Visitor Data**

Technical data (logs, analytics) is stored for a short term — usually several months — unless otherwise required by law. Analytical data may be kept longer in aggregated, anonymized form. Cookies on your device are retained based on their individual lifespan (see Section 7), unless you delete them manually.

Once the retention period expires, the relevant personal data is securely deleted or anonymized so that it can no longer be associated with any individual. We use secure deletion methods to ensure that data cannot be recovered.

Eduvance Limited has implemented internal policies that regulate retention timelines for each data category. We periodically review stored data and delete information that is no longer justified by business or legal necessity.

If you would like to know the specific retention period for your personal data, feel free to contact us (see Section 17).

**11. Data Protection and Security Measures**

We implement appropriate technical and organizational measures to ensure the security of personal data and to protect it from breaches, unauthorized access, misuse, alteration, or destruction. Eduvance Limited regularly reviews and enhances these measures in line with evolving technologies and emerging risks.

Key Safeguards Implemented by the Company Include:

 • Encryption

Sensitive personal data is encrypted during transmission (e.g., HTTPS/TLS for website and email communication) and, where applicable, at rest (e.g., in databases or storage systems). This ensures that even in the event of interception or device compromise, the content remains inaccessible without the decryption key.

 • Access Controls

Access to personal data is strictly limited on a need-to-know basis. Only authorized employees or contractors who require data access for work purposes may access it. We use user authentication (e.g., passwords, two-factor authentication) and role-based access controls to ensure individuals only see the data necessary for their role. Highly sensitive data (e.g., financial records, HR documents) is subject to additional protection and oversight by management or the DPO.

 • Backups and Disaster Recovery

We conduct regular encrypted backups of key data and store them securely to prevent data loss due to technical failure or emergency. These backups are periodically tested to ensure system recovery capabilities in case of incidents.

 • Monitoring and Security Audits

Our information systems are continuously monitored for suspicious activity and unauthorized access attempts. We use intrusion detection tools and antivirus protection to identify and block threats. Internal and external audits are conducted to assess the effectiveness of our security practices and detect vulnerabilities. Audit findings are reviewed by management and guide security enhancements.

 • Physical Security

Where data is stored in physical form or on local servers, we ensure physical safeguards. Company premises are locked and monitored; sensitive paper documents are stored in secured cabinets or safes; and access to data processing areas is restricted to authorized personnel. Physical records are securely destroyed when no longer needed.

 • Employee Training and Confidentiality

Employee awareness is a key security factor. All employees of Eduvance Limited undergo mandatory training in data protection and information security. They are educated on UK GDPR requirements, company procedures, secure handling practices, and incident reporting protocols. Refresher trainings and policy updates are regularly issued. All employees, contractors, and interns with access to personal data must sign confidentiality agreements and comply with this policy. Compliance is monitored, and violations are subject to disciplinary or legal action (see Section 12).

We also adopt Privacy by Design and Privacy by Default principles, meaning that privacy requirements are embedded into the planning of all our systems, processes, and services, with the most privacy-friendly settings enabled by default.

While no data transmission or storage method is 100% secure, we continuously improve our protection systems and respond promptly to new threats. If you suspect a data compromise or vulnerability, please contact us immediately (see Section 17) — we highly value security-related feedback.

**12. Employee and Partner Responsibilities**

All employees and engaged specialists who have access to personal data within Eduvance Limited are personally responsible for adhering to the requirements of this Privacy Policy and ensuring data confidentiality. The Company has implemented internal regulations that clearly define the obligations of individuals handling personal data. Key responsibilities of employees and partners include:

**Compliance with Policies and Procedures**

Each employee is required to fully comply with this Privacy Policy and all related internal information security protocols. Partners and contractors processing data must adhere to equivalent rules, as stipulated in their agreements with the Company.

**Confidentiality and Access Minimization**

Employees must maintain the confidentiality of personal data and use it strictly for work-related purposes. Disclosure or transmission of personal data to colleagues or third parties is prohibited unless explicitly authorized and necessary. Staff must observe the principle of data minimization — not collecting, copying, or storing more data than necessary.

**Secure Handling of Data**

Personal data must be handled securely. Employees are required to use corporate systems and tools (e.g., secure computers, emails, storage solutions) and must avoid saving work-related personal data to personal, unencrypted devices or sharing it through unauthorized channels.

**Prompt Incident Reporting**

If an employee suspects or becomes aware of a personal data security incident (e.g., lost laptop containing personal data, misdirected email, account breach), they must immediately notify Company leadership and/or the Data Protection Officer (DPO). Prompt reporting is essential to limit the risk and fulfill legal notification requirements (see Section 13).

**Training and Awareness**

Employees must participate in all assigned training programs on data protection and security, and are expected to stay informed about updated policies. They are encouraged to consult management or the DPO if uncertain about proper practices.

Violation of these responsibilities is considered a serious offense. Disciplinary measures — up to and including dismissal — may apply. If a violation results in a data breach or legal non-compliance, it may also be reported to supervisory authorities, and legal liability may follow.

As for our partners and suppliers with data access, their obligations are contractually defined. We require that they maintain security standards no lower than our own. In the event of a breach or non-compliance by a partner, they are contractually and legally liable. Eduvance Limited reserves the right to terminate the partnership and seek compensation for damages.

**13. Data Breach Response**

Eduvance Limited takes every precaution to safeguard personal data, but we recognize that security incidents can occur. A personal data breach is defined as a security violation that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. The Company has an established incident response plan, which includes the following steps:

**1. Immediate Containment and Assessment**

Upon identifying a potential breach, the designated personnel (e.g., the DPO or IT Security Team) immediately assess the nature and scope of the incident. Priority is given to containing the issue: disconnecting compromised systems, suspending unauthorized access, or fixing vulnerabilities. Simultaneously, information about the event is gathered.

**2. Notification to Supervisory Authorities**

If a data breach poses a risk to the rights and freedoms of individuals, the Company will notify the appropriate supervisory authority. In the UK, this is the Information Commissioner’s Office (ICO).

In accordance with UK GDPR, such notification must occur within 72 hours of the Company becoming aware of the breach. The report includes:

 • the nature of the breach

 • types of personal data involved

 • number of individuals affected

 • potential consequences

 • measures taken to address the breach

If all information is not available within 72 hours, a preliminary report is submitted with follow-ups as details emerge.

**3. Notification to Affected Individuals**

If the breach is likely to result in a high risk to the rights and freedoms of data subjects (e.g., exposure of financial information or credentials), we will inform affected individuals as soon as possible.

The notification will include:

 • a description of the breach

 • the types of data involved

 • recommended steps to minimize risk (e.g., password changes, fraud monitoring)

 • contact details for further questions

Where individual notification is disproportionately difficult (e.g., thousands of users affected), we may use public notices or other equally effective methods.

**4. Investigation and Remediation**

A thorough internal investigation is conducted to determine the cause of the breach. Depending on the findings, we implement corrective measures such as strengthening system security, updating protocols, or providing additional employee training.

All incidents are documented, and findings are reviewed by Company management. When applicable, we cooperate with law enforcement to hold malicious actors accountable.

Eduvance Limited follows a policy of transparency. Where feasible, we keep data subjects informed about the resolution of the incident and the actions taken to safeguard their information.

Data breaches are treated as serious incidents that may damage our reputation and client trust — therefore, we prioritize swift, effective, and responsible responses to all such events.

**14. Data Subject Rights**

In accordance with the UK GDPR, the Data Protection Act 2018, and other applicable laws, individuals (data subjects) have several important rights regarding their personal data. Eduvance Limited respects these rights and ensures mechanisms are in place to facilitate their exercise. Your rights include:

**Right of Access**

You have the right to know whether the Company processes your personal data, and if so, to access that data. This includes receiving confirmation of processing and a copy of your personal data, as well as information about the purposes of processing, data categories, third-party recipients, retention periods, and your rights.

*The first copy is provided free of charge. For additional copies, a reasonable fee may apply.*

**Right to Rectification**

If you believe that any personal data we hold about you is inaccurate, incomplete, or outdated, you have the right to request correction or supplementation. We will promptly make the necessary changes and inform you of the update. In some cases, we may request documentation to verify the updated information (e.g., a passport copy to correct your name or date of birth).

**Right to Erasure (“Right to be Forgotten”)**

You may request deletion of your personal data in specific circumstances, including:

 • the data is no longer needed for its original purpose

 • you withdraw consent, and no other legal ground exists

 • you object to processing and we have no overriding legitimate grounds

 • the data was processed unlawfully

 • deletion is required by law

**Note:** This right is not absolute. We may be legally required to retain certain data (e.g., for accounting, legal claims, or compliance). If we cannot erase your data, we will explain the lawful basis for continuing to store it. Where deletion is possible, we will also inform any third-party recipients to delete copies of the data.

**Right to Restrict Processing**

You may request that we restrict the processing of your personal data (other than storage) in the following cases:

 • you contest the accuracy of the data (processing is paused during verification)

 • processing is unlawful, and you oppose deletion

 • we no longer need the data, but you require it to establish or defend legal claims

 • you object to processing, pending verification of our legitimate grounds

During restriction, we will not process the data for other purposes without your consent or legal justification. You will be informed before any restriction is lifted.

**Right to Data Portability**

You have the right to receive the personal data you provided to us in a structured, commonly used, machine-readable format (e.g., CSV), and to request direct transfer to another service provider where technically feasible.

*This applies only to data processed based on your consent or contract, and by automated means.*

**Right to Object**

You may object at any time to the processing of your personal data if the basis is our legitimate interest or that of a third party.

If you object, we must cease processing unless we demonstrate compelling legitimate grounds that override your rights, or the data is necessary for legal claims.

You also have the absolute right to object to processing for direct marketing purposes. Upon receiving such an objection, we will immediately stop using your data for that purpose.

**Right to Withdraw Consent**

Where processing is based on your consent, you have the right to withdraw that consent at any time. Upon withdrawal, we will stop the related processing as soon as possible. Withdrawal does not affect the lawfulness of processing already performed based on your prior consent.

**Right Not to Be Subject to Automated Decisions**

You have the right not to be subject to decisions made solely by automated means — including profiling — that produce legal effects or similarly significant impacts.

Eduvance Limited does not currently make significant decisions through fully automated processing without human involvement. If this changes, you will have the right to request human intervention, express your views, and contest the decision.

**How to Exercise Your Rights**

You can submit your request to exercise any of these rights by email or postal mail (see Section 17: Contact Information). Please include identifying details so we can verify your identity and process your request securely. If acting through a representative, supporting documents proving authorization will be required.

We will respond to valid requests within one month of receipt. In complex cases, we may extend the period by up to two months and will notify you of the reason for any delay.

We may refuse a request only in limited cases as permitted by law — in such cases, we will explain the legal reason and your further options.

If you believe your rights have been violated, you also have the right to file a complaint with the Information Commissioner’s Office (ICO) or your local supervisory authority. Contact details for the ICO are available on its official website.

However, we encourage you to contact us first — we will do our best to resolve your concerns promptly and fairly.

**15. Children’s Data**

Eduvance Limited is committed to protecting the privacy of minors. While our educational programs and website are primarily intended for adult users, we recognize that minors (e.g., older schoolchildren or college students) may participate in certain training programs. We take additional precautions to ensure the safe and lawful processing of personal data for individuals under 18 years of age.

**Parental or Guardian Consent**

If a data subject is under 18 years of age, we recommend that their personal data be provided with the knowledge and supervision of a parent or legal guardian.

For children under the age of 13, we do not knowingly collect or process personal data without verifiable consent from a parent or legal guardian. Where a child under 13 wishes to use our online services, parental consent is mandatory. We take reasonable steps to verify such consent (e.g., confirmation via email or phone).

**Limiting the Scope of Data Collection**

We intentionally avoid requesting any unnecessary personal data from children. When a child participates in a training program, our communication and administration is generally conducted via the parent or guardian.

The personal data we collect from children is minimal and limited to what is strictly required — e.g., name, age, parent’s contact details, attendance records, and achievement results. We do not engage in any form of marketing targeted at minors.

**Parental Control and Rights**

Parents or legal guardians may exercise data subject rights on behalf of their child (see Section 14), including access, correction, or deletion of data — unless there is a legal obligation to retain the data (e.g., educational records).

If a child is of legal age to consent independently (13 and older for online services in the UK), we consider the child’s wishes, but may also require parental involvement in unclear cases.

**Online Safety for Children**

We make every effort to ensure our website content is appropriate for a general audience and does not include harmful material. Our services are not specifically directed at young children without institutional or parental involvement.

If we conduct surveys, contests, or educational campaigns involving minors, we explicitly state age requirements and participation conditions that comply with applicable law (e.g., requiring parental contact details).

If we become aware that we have received personal data from a child under 13 without verified parental consent, we will take steps to delete such information. We encourage parents to monitor their children’s online activity and educate them about privacy and safety online.

**16. International Operations and Multilingual Support**

**Global Presence**

Eduvance Limited is a UK-registered company, but our operations and audience extend beyond a single country. We may offer educational programs and services in cooperation with international partners or through affiliated entities abroad.

If the Company maintains official representations or branches in other jurisdictions, those entities are bound by this Privacy Policy and the applicable laws of their respective countries.

Regardless of where data processing takes place, Eduvance Limited guarantees a consistent and high standard of data protection. Uniform internal standards and procedures apply throughout the organization, and cross-border data transfers are governed by legal contracts and protective mechanisms (see Section 9).

This means your data remains secure and protected even if, for example, it is processed by an overseas office of the Company.

We actively monitor changes in international data privacy laws (e.g., new regulations in the EU, US, or Asia) and adjust our practices accordingly to maintain full compliance.

**Multilingual Accessibility**

We recognize that our users may speak different languages, and we strive to support multilingual communication. This applies both to the languages used in our educational programs and to the availability of information about the Company.

This Privacy Policy may be translated into other languages for the convenience of international users. If another language is more understandable to you, you may request a translated version of this document or view it on our website (if available).

**Note:** As this Policy is a legal document, in the event of any discrepancies between language versions, the English version shall prevail, unless otherwise required by the laws of a specific jurisdiction.

We take care to ensure accurate translations and aim to keep all language versions up to date, but for legal clarity, we recommend referring to the official English version.

We also accept communications in multiple languages. You may contact us regarding your personal data in English, Russian, or another language you speak — we will do our best to respond in that language or provide a translated reply.

Our international team is committed to removing language barriers that could hinder the exercise of your data rights.

**17. Contact Information**

If you have any questions, comments, or requests related to this Privacy Policy or the processing of your personal data by Eduvance Limited, please contact us using one of the following methods:

**Eduvance Limited**

**Company Number:** 15426004

167–169 Great Portland Street, 5th Floor

London, W1W 5PF, United Kingdom

 **• Email:** privacy.eduvance@outlook.com

 **• Phone:** +49 (0) 172 911 6761 (international contact number)

You may direct your inquiry specifically to our Data Protection Officer (DPO) by using the same contact details and addressing your message to “DPO” or “Privacy Team.”

We recommend using email for requests related to the exercise of data subject rights, as this enables us to process your inquiry more quickly and securely.

The London address is our official mailing address — you may send formal requests or correspondence by post. Please mark the envelope with “FAO: Data Protection Officer” to ensure proper handling.

We are committed to responding to all lawful requests in a timely and thorough manner. If your inquiry concerns the exercise of your rights (see Section 14) or a request for additional information about your data, please provide sufficient identifying details so we can locate your records and respond accordingly.

**18. Updates to the Policy**

This Privacy Policy may be revised and updated by Eduvance Limited from time to time to reflect changes in our activities, legal requirements, or the adoption of new technologies. We are committed to transparency regarding any material changes made to this Policy.

**Effective Date of Changes**

The updated version of the Policy will be published on our website (at the same address as the previous version or in the “Privacy Policy” section) and will bear a new effective date.

We recommend that you review this document periodically to stay informed about our current data processing practices. The effective date is indicated at the top of the Policy.

**Notification of Significant Changes**

If we make changes that significantly affect your rights or the way we process your personal data (e.g., changing processing purposes or adding new categories of data recipients), we will make reasonable efforts to notify you.

Such notification may include:

 • a direct email (if we have your email address), or

 • a prominent banner on our website before the changes take effect.

In some cases, where legally required, we may request your renewed consent for new processing activities.

**Continued Use of Services**

Your continued use of our services or website after publication of an updated Privacy Policy constitutes your acceptance of the changes, to the extent permitted by law.

However, no changes will be applied retroactively — we will not use your previously collected personal data for new purposes without your prior consent if required.

If you have questions or concerns regarding any changes to the Policy, we encourage you to contact us before the updates take effect (see Section 17). Your trust is important to us.

**Thank you for taking the time to review Eduvance Limited’s Privacy Policy.**

We value the trust you place in us when sharing your personal information, and we are fully committed to protecting your data through responsible, secure, and transparent practices.