UK GDPR Policy

1. Policy statement

Trust Education ("the Company") is a UK-based education recruitment business providing work-finding services to schools, academies, nurseries, colleges and other education providers, and to work-seekers and temporary workers across the UK. We process personal data so that we can deliver these services and, in doing so, act as a data controller.

We are committed to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and all other applicable data protection laws. This policy sets out the principles, roles and responsibilities that apply to all personal data processed by or on behalf of Trust Education.

Trust Education puts people at the forefront of everything we do, and that includes respecting the privacy and data protection rights of candidates, temporary workers, employees, clients, pupils and all other individuals whose data we handle.

2. Purpose of this policy

The purpose of this policy is to:

- Set out how Trust Education complies with UK GDPR and embeds the data protection principles in its day-to-day operations.
- Provide a framework for staff and others acting on our behalf when handling personal data.
- Support and complement the Privacy Notice, Data Retention Policy and Data Protection Policy, which provide further detail on how we collect, use, share and retain personal data.

This policy is supported by more detailed procedures (for example, data breach response and subject access procedures).

3. Scope

This policy applies to:

- All personal data processed by or on behalf of Trust Education, in any format (electronic, paper, audio, visual or otherwise).

- All groups of data subjects, including but not limited to: candidates and temporary workers; employees and directors; clients and their staff; pupils and parents/carers; referees and emergency contacts; suppliers and other business contacts.
- All Trust Education workers, including employees, directors, temporary workers engaged through us, consultants, agency workers and contractors who access our systems or handle personal data.

The policy covers all processing carried out in connection with Trust Education's work-finding, payroll, compliance, safeguarding and business support activities. We only provide roles within the UK; we do not routinely transfer personal data outside the UK/EEA (see section 10).

4. Key definitions

For the purposes of this policy:

- Personal data: Any information relating to an identified or identifiable living individual.
- Special category data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for identification purposes, health data or data concerning a person's sex life or sexual orientation.
- Criminal offence data: Personal data about criminal convictions or offences (including DBS information).
- Processing: Any operation performed on personal data, including collection, recording, storage, use, sharing, alteration, retrieval, disclosure or destruction.
- Data subject: The living individual to whom the personal data relates.
- Controller: The organisation that determines the purposes and means of processing personal data (Trust Education).
- Processor: An organisation that processes personal data on behalf of the controller.

5. Roles and responsibilities

The following roles and responsibilities apply:

5.1 Directors

The Directors have overall responsibility for ensuring compliance with data protection legislation and approving this policy.

5.2 Data Protection Officer (DPO)

The Data Protection Lead is responsible for day-to-day oversight of data protection compliance, advising on data protection issues, co-ordinating responses to data subject requests, and managing data breach investigations and notifications.

5.3 Managers

Managers must ensure staff in their teams understand and follow this policy and related procedures, and that appropriate technical and organisational measures are in place in their areas.

5.4 All staff and workers

Everyone who works for or with Trust Education is responsible for:

- Handling personal data in line with this policy and their training.
- Reporting actual or suspected data breaches without delay.
- Following security and confidentiality requirements set by Trust Education and client schools, including those set out in the Candidate Induction Booklet.

5.5 Processors and other third parties

Third-party processors (for example, payroll providers or IT service providers) must only process personal data on our documented instructions and must provide sufficient guarantees regarding security and compliance. Appropriate written agreements must be in place before any processing begins.

6. UK GDPR principles

Trust Education will process personal data in accordance with the six core principles of UK GDPR, plus the overarching principle of accountability:

- Lawfulness, fairness and transparency: We will only process personal data where we have a valid lawful basis, will treat individuals fairly, and will be open and transparent about how we use personal data.

- Purpose limitation: We will collect personal data only for specified, explicit and legitimate purposes and will not use it in ways that are incompatible with those purposes.

- Data minimisation: We will ensure that personal data is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

- Accuracy: We will take reasonable steps to keep personal data accurate and, where necessary, up to date, and will correct or delete inaccurate information without undue delay when notified.

- Storage limitation: We will not keep personal data for longer than necessary. Retention periods are set out in our Data Retention Policy and related schedules.

- Integrity and confidentiality (security): We will process personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical and organisational measures.

- Accountability: We are responsible for, and must be able to demonstrate, compliance with these principles. We do this through policies, training, records of processing activities, contracts, audits and other controls.

7. Lawful bases for processing

Trust Education will always identify and document a lawful basis before processing personal data. In line with our Privacy Notice, we rely on the following lawful bases:

- Consent – for example, for certain marketing communications. Individuals may withdraw consent at any time.
- Legitimate interests – where processing is necessary for our legitimate business interests (such as managing our candidate database, providing work-finding services and developing client relationships) and these are not overridden by the individual's rights.
- Legal obligation – where processing is necessary to comply with legal or regulatory requirements.
- Contract – where processing is necessary for us to enter into or perform a contract with an individual.

Where we process special category data or criminal offence data (for example, health information or DBS results), we will ensure that an additional condition under UK GDPR and the Data Protection Act 2018 is met – for example, processing necessary for employment and social protection law, for reasons of substantial public interest linked to safeguarding, or on the basis of explicit consent.

8. Rights of individuals

Trust Education will respect and facilitate the following rights of data subjects under UK GDPR:

- Right to be informed about how their personal data is used.
- Right of access to their personal data.
- Right to rectification of inaccurate or incomplete personal data.
- Right to erasure ("right to be forgotten"), in certain circumstances.
- Right to restrict processing, in certain circumstances.
- Right to data portability, in certain circumstances.
- Right to object to processing based on legitimate interests.
- Rights in relation to automated decision-making and profiling.
- Right to withdraw consent at any time where processing is based on consent.

Requests to exercise these rights should be referred promptly to the Data Protection Lead. We will respond within the statutory time limits and in accordance with our internal procedures.

9. Data protection by design and default

We will embed data protection into the design of our processes, systems and services by:

- Considering privacy and data protection risks at the outset of new projects, systems or services.
- Limiting access to personal data to those who need it for their role.
- Implementing role-based access controls and strong authentication.
- Pseudonymising or anonymising personal data where feasible.

Where a type of processing is likely to result in a high risk to individuals' rights and freedoms, we will carry out a Data Protection Impact Assessment (DPIA) in line with ICO guidance.

10. Data sharing, disclosures and transfers

We share personal data only where necessary, lawful and proportionate.

10.1 Routine sharing

In order to provide work-finding services and manage our business, we may share personal data with:

- Client schools and other education providers in the UK.
- Former employers or referees.
- Payroll providers and other payment intermediaries.
- Other recruitment agencies in the supply chain.
- Professional advisers, auditors and regulators.

10.2 International transfers

Trust Education does not routinely transfer personal data outside the UK/EEA. If a transfer outside the UK/EEA is necessary, we will ensure that appropriate safeguards are in place, such as an adequacy decision, International Data Transfer Agreement (IDTA) or other approved mechanisms, and that data subjects are informed through our Privacy Notice.

10.3 Data sharing agreements

Where appropriate, data sharing or processing agreements will be put in place to clarify roles, responsibilities and data protection obligations.

11. Data security

Protecting the confidentiality, integrity and availability of personal data is essential to safeguarding pupils, staff and others, and to maintaining trust in Trust Education and our partner schools.

We will maintain appropriate technical and organisational measures, which may include:

- Secure configuration, firewalls, anti-virus and patch management on our systems.
- Access controls and user authentication; unique log-ins; strong passwords.
- Encryption of laptops and mobile devices where feasible.
- Secure storage of paper files in locked cabinets or secure offices.
- Regular back-ups and business continuity arrangements.
- Confidential waste disposal via shredding or approved contractors, in line with the Data Retention Policy.

All staff and workers must:

- Lock their computer screens when away from their desks and avoid displaying personal data where it can be seen by unauthorised people.
- Never share log-in details or passwords.
- Keep confidential or personal data out of the body of emails where possible, and use password-protected attachments with passwords sent separately.
- Use school shredders or secure shredding boxes for any paper records that are no longer required.
- Be vigilant about phishing and other suspicious emails and report them to the appropriate contact within Trust Education or the client school.

12. Data breaches and incident reporting

A personal data breach is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All staff and workers must:

- Report any actual or suspected personal data breach immediately to the Data Protection Lead and, where applicable, the school's Data Protection Officer.
- Provide all relevant information to enable investigation, including what data is involved, who is affected, how the incident occurred and what steps have been taken so far.

Trust Education will:

- Investigate all reported incidents promptly.
- Take appropriate steps to contain and remedy the breach.
- Assess the risk to individuals and determine whether the breach must be notified to the Information Commissioner's Office (ICO) and/or affected individuals. The ICO must be notified within 72 hours of becoming aware of a notifiable breach.

Records of all data breaches, whether or not they require notification, will be maintained.

13. Records management and retention

We will keep records of our processing activities and retain personal data only for as long as necessary for the purposes for which it was collected, or to meet legal, regulatory or contractual requirements.

Retention periods for different categories of records are set out in Trust Education's Data Retention Policy and supporting schedules. At the end of the relevant retention period, personal data will be disposed of securely so that it cannot be reconstructed or retrieved.

14. Training and awareness

All staff and workers who handle personal data must:

- Complete appropriate data protection and information security training at induction and at regular intervals thereafter.
- Familiarise themselves with this policy, the Data Protection Policy, the Privacy Notice, the Data Retention Policy and relevant client school policies.

Additional or refresher training will be provided following significant changes to data protection law or to Trust Education's processes.

15. Monitoring and review

Compliance with this policy may be monitored through audits, spot checks and reviews of data protection practices.

This policy will be reviewed at least annually, and earlier if there are significant changes in legislation, ICO guidance, REC guidance or the nature of Trust Education's activities. Any updates will be approved by the Board and communicated to relevant staff, and the version number and date in the footer will be updated accordingly.