Estu

Estu Global Ltd

Privacy Policy

Introduction

Estu is committed to protecting learners' privacy. This Policy governs Estu's data collection, processing and usage practices and describes learner choices regarding use, access and correction of your personal information. This Privacy Policy explains how the Estu uses information about current and prospective customers and learners.

Our Privacy Policy explains:

- The basis for the lawful processing of personal data.
- The information Estu collect about its learners.
- How Estu uses learner information.
- Access to learner information, correction, retention, and deletion.
- Sharing personal data.
- Changes to our privacy policy.

Basis for lawful processing of personal data

The legal basis for the collection and processing of personal data is:

- For administration: which is necessary to fulfil service requests.
- Where consent is provided or processing may be necessary, to comply with legal obligations.
- Where explicit consent has been provided for processing sensitive data.
- When legally required by the Education and Skills Funding Agency (ESFA) and or other relevant authority.

The information Estu collects and processes

As an Ofsted regulated provider, internal data governance is a top priority. Estu collects and processes learners' personal data when they enrol on a programme (including in some cases full name, contact details, date of birth and National Insurance number), when they participate in learning activities and when a learner provides feedback. We have a legal responsibility to ensure the collection and process of personal data follows regulations including the UK General Data Protection Regulation (GDPR).

How Estu uses Learner's information

Estu only collects what is needed for the delivery and for funding and auditing purposes of the programme a learner is enrolling on.

This information helps us to tailor our programmes to suit learning needs, evidence the training a learner has received, and demonstrate to auditors and qualification awarding organisations that compliance and quality requirements are met.

In order to deliver some contracts, for example those aligned to public funding, Estu will be required to provide personal data to a limited number of organisations involved in the delivery of an apprenticeship or adult learning programme, such as its technology suppliers, the ESFA, Ofsted and the relevant qualification awarding organisations.

Estu are required by the ESFA to retain personal information for seven years for auditing and funding purposes. This is stored securely and fully deleted from our systems once this time has passed.

Estu will not use or share information for marketing purposes except to offer other educational and progression opportunities.

Access to information, correction, retention, and deletion

A learner has the right to request a copy of the information that Estu holds about them. If a learner would like a copy of some or all personal information, please email or write to us at the address below.

Estu wants to ensure personal information is accurate and up to date. A learner may ask us to correct or remove information a learner thinks is inaccurate.

For learners who have started one of our programmes, Estu will not be able to remove personal data for seven years due to contractual, auditing and compliance purposes.

Sharing Learners' personal data

Estu may need to share learners' personal data with our employees, agencies, suppliers (including any intermediaries or other product providers involved in the delivery of training) for the following purposes:

1. To deliver and administer training.
2. For staff training.
3. Quality assurance.
4. To fulfil a statutory/legal obligation.
5. For safeguarding, or health and safety purposes.
6. To determine what training a learner may benefit from in the future.
7. To offer other educational and career progression opportunities.

Estu may also share recordings of workshops with other learners to enable non-attendees to access material for educational purposes.

Estu would use personal data in any legal proceedings. Estu are required by law to disclose personal data to law enforcement agencies in connection with any investigation to prevent unlawful activity.

Estu will never disclose personal data to any third parties for the purposes of marketing.

Measures to enable us to meet our data protection obligations

Data breach management

Our Data Protection Officer (DPO) oversees the breach notification process, ensuring regulatory requirements are met.

The procedure summary below (and illustrated in fig.1), outlines Estu's data breach notification process:

1. Detection of breach: Any employee who detects a potential data breach immediately reports it to the programme lead within Estu.
2. Initial Assessment:
    - The programme lead completes an initial assessment to determine the scope, nature, and severity of the breach.
    - This assessment includes gathering relevant information such as the type of data involved, the cause of the breach, and the potential impact on data subjects.
3. Notification to Estu's DPO: If the breach is confirmed or suspected to involve personal data, the programme lead notifies our DPO.
4. Estu DPO assessment:
    - Estu's DPO assesses the breach in detail, evaluating the scale of the incident, sensitivity of the data affected, and the potential risks to data subjects' rights and freedoms.
    - They determine whether the breach is reportable to the Data Controller based on UK GDPR criteria.
5. Notification to Data Controller: If the breach meets the criteria for notification under UK GDPR, Estu's DPO promptly notifies the Data Controller. The notification includes all relevant details of the breach, such as the nature of the breach, the categories of data affected, the potential consequences, and any measures taken or proposed to address the breach.
6. Collaboration with Data Controller: Estu will then work closely with the Data Controller to investigate the breach, assess its impact, and implement remedial actions. This may involve sharing additional information, conducting joint

investigations, and coordinating response efforts to mitigate the effects of the breach.

7. Documentation and reporting:
    - Throughout the process, records are maintained documenting all aspects of the breach, including initial reports, assessments, communications, and remediation efforts.
    - Estu's DPO will be responsible for ensuring that all documentation is prepared and submitted in accordance with UK GDPR requirements.
8. Follow-Up and monitoring: Following the breach notification, Estu's DPO, and as appropriate programme lead, will monitor the situation closely, assessing any ongoing risks or impacts on affected individuals.
9. Review and lessons learned: After the breach has been addressed, Estu will facilitate a review meeting to evaluate the effectiveness of our response and identify any areas for improvement. Any improvement or process updates will be reflected in our Operations Plan.

Assistance with GDPR Compliance

In the unlikely event of a personal data breach, and where Estu is the data processor, our team will assist the Data Controller in meeting its obligations under the GDPR. This includes establishing shared points-of-contact (POCs) between organisations, agreeing a cadence of regular touchpoints to communicate data risks and mitigations Estu is taking. Our DPO oversees and reviews these communication channels and ensures that all regulatory requirements are met.

Compliance with Data Subject Rights

Estu is committed to upholding the rights of data subjects, as outlined in the GDPR. Our procedures to facilitate the exercise of these rights include mechanisms for receiving access requests through designated channels, which are then reviewed and actioned by authorised personnel within our organisation. These requests are logged and tracked through a centralised system.

Consent Management

Where consent is required for data processing activities, Estu adheres to standards of active, informed consent as stipulated by the GDPR. We maintain auditable records of consent, including details of how and when consent was obtained, the purposes for which it was obtained, and any relevant disclosures provided to data subjects.

Legal Safeguards for Data Transfers

In the event that personal data transfers outside of the UK become necessary, we will ensure that appropriate legal safeguards are in place to legitimise these transfers in accordance with the GDPR.

Records of Processing Activities

We maintain records of processing activities as required by the GDPR. These records include details such as the purposes of processing, categories of personal data processed, data sharing arrangements, retention periods, and security measures implemented.

Regular Testing and Evaluation

Our records are reviewed at minimum annually, and updated to reflect changes in processes and regulatory requirements with the GDPR, ensuring transparency and accountability. This

includes internal audits, vulnerability assessments, and reviews of our policies, procedures, and technical controls.

Implications for Estu Operations

- Ensure Estu follow the legal requirements of collecting, processing and sharing learners' data.
- Ensure this privacy policy is circulated with everyone associated with Estu and that any concerns surrounding this policy are raised and resolved.
- Mandatory data privacy policy training for all Estu staff.

Estu maintains a comprehensive set of technical and organisational measures to uphold the confidentiality, integrity, and availability of personal data processed. This includes regular risk assessments, encryption protocols, access controls, and cybersecurity measures.

All Estu staff involved in processing personal data receive regular training on data protection and information security.

To preserve data confidentiality and integrity, Estu utilise individual SharePoint sites to ensure robustly managed access rights, guaranteeing that only relevant users have access to Learners' personal data.

All new starters with Estu complete an induction on Estu's data policies, consent processes, and data management guidelines with our data protection officer (DPO).

Continuous Improvement

Estu is committed to a culture of continuous improvement in its data management practices. This includes staying abreast of developments in data protection legislation, incorporating feedback from learners and staff, and actively participating in relevant training and initiatives that enhance our ability to effective manage data in line with UK GDPR.

All of our data management processes and policies are reviewed as a minimum annually, or when there is a change to legislation or guidance, to ensure compliance with these standards. Reviews are led by Estu's Data Protection Officer (DPO) and Chief Operating Officer (COO), and signed off by Estu's board.

Key roles

Data Protection Officer (DPO): Anne-Marie Smith

Email: anne-marie.smith@estuglobal.com