



Estu Global Ltd

Privacy & Data Protection Policy

v3



Policy version control

Issue	Date	Approved By	Position	Revision Notes
V1				New policy
V2	Feb 24	Bruce Storey	COO	Update and revision
V2.1	Oct 24	Bruce Storey	COO	Updated to confirm workshop recording responsibilities
V2.2	Feb 25	Bruce Storey	COO	Reviewed and dated
V3	Feb 26	Bruce Storey	COO	• Contents page added • Revised introduction • Update to DPO role and responsibilities • Update to Basis for lawful processing of personal data section • Update to recordings of workshops • Update to data breach management regarding where Estu is the Data Controller • Expanded section on Compliance with data subject rights • Added AI / automated tools wording
Next Review Date: Feb 27			Policy Owner: COO	

Privacy and Data Protection policy

Contents

Policy version control	2
Privacy and Data Protection policy	3
Introduction	4
Policy objectives.....	4
Roles and responsibilities.....	5
Basis for lawful processing of personal data.....	5
The information Estu collects and processes.....	6
How Estu uses learner’s information	6
Access to information, correction, retention, and deletion.....	7
Sharing learners’ personal data	7
Measures to enable us to meet our data protection obligations	8
Implications for Estu operations	11
Continuous improvement	11
Key roles.....	13
Related policies and documents	13

Introduction

Estu is committed to protecting the privacy and personal data of learners, prospective learners, staff, job applicants, associates, tutors, employer/client contacts, suppliers and other stakeholders. This Policy sets out how Estu collects, uses, stores, shares and protects personal data in accordance with UK data protection legislation. This Privacy Policy explains how Estu uses information about current and prospective learners, employer clients and other stakeholders.

This document operates as Estu's internal Privacy & Data Protection Policy. Estu may also issue privacy notices to learners, staff, applicants, employers and other stakeholders explaining how their personal data is used in specific contexts.

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.

Policy objectives

The purpose of this policy is to achieve the following:

- To fully comply with all relevant data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, ensuring lawful, fair, and transparent processing of personal data.
- To protect the privacy and security of personal data belonging to learners, staff, and other stakeholders by implementing appropriate technical and organisational measures to prevent data breaches, loss, or misuse.
- To ensure that individuals are fully informed about how their personal data is collected, used, stored, and shared, providing clear information on their rights under data protection laws.
- To collect and retain only the personal data necessary for the organisation's operations, and to ensure that data is kept accurate, up-to-date, and only for as long as necessary, in line with legal and business requirements.
- To ensure that personal data is shared with third parties only where necessary and lawful, with appropriate contracts and safeguards in place to protect the data when shared with partners, contractors, or external bodies.

Roles and responsibilities

- **Data Protection Lead / Data Protection Officer (DPO):** Responsible for overseeing implementation of this Policy, coordinating data protection compliance, managing data subject rights requests, maintaining data protection records, supporting breach assessment and notifications, and advising staff on appropriate handling of personal data.
- **Chief Operating Officer (COO):** Works alongside the DPO to ensure that the organisation adheres to all data protection regulations, leading regular reviews of data management practices and signing off on compliance-related decisions. The COO also plays a key role in ensuring all staff receive appropriate data protection training.
- **Line Managers:** Responsible for ensuring that their teams follow data protection guidelines, raising any data security concerns, and supporting the DPO and COO in maintaining compliance within their departments.
- **All Employees:** Expected to handle personal data responsibly, comply with all data protection procedures, report any breaches or concerns, and complete mandatory data protection training. All staff must ensure data is processed lawfully and in accordance with internal policies.

Basis for lawful processing of personal data

Estu will identify and document an appropriate lawful basis before processing personal data. Depending on the activity, this may include:

- Performance of a contract, for example delivering a learning programme or service
- Compliance with a legal obligation, for example funding, audit, safeguarding, tax, employment or regulatory requirements
- Legitimate interests, for example managing employer/client relationships, quality assurance, service improvement and appropriate business communications
- Consent, where this is required and appropriate, for example certain optional communications or use of images/testimonials
- Explicit consent or another UK GDPR Article 9 condition where special category data is processed.

Special category data

Estu may process special category data where necessary and lawful, for example information

relating to health, disability, learning support needs, reasonable adjustments, safeguarding, equalities monitoring or employment matters. Such data will be processed only where an appropriate lawful basis and special category condition applies, and access will be restricted to those who need it for their role.

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).

Estu may also process personal data relating to staff, job applicants, associates, tutors, employer/client contacts, suppliers and other stakeholders where necessary for employment, contracting, programme delivery, governance, quality assurance, compliance, safeguarding, finance, marketing or relationship management purposes.

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.

Individuals may contact Estu's Data Protection Lead / DPO with questions or concerns about how their personal data is handled. Individuals also have the right to raise a concern with the Information Commissioner's Office where they are unhappy with how their personal data has been handled.

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. Recordings of workshops can be made only by Estu personnel and not by any other parties, including other workshop attendees.

Where workshops are recorded, learners and attendees will be informed in advance or at the start of the session. Recordings will be used only for legitimate educational, quality assurance or programme administration purposes, stored securely, shared only with appropriate participants or staff, and retained only for as long as necessary.

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.

Where Estu shares personal data with suppliers, platforms, contractors or other processors, Estu will take proportionate steps to ensure that appropriate contractual, confidentiality and

security arrangements are in place. This includes considering access controls, data location, retention, breach reporting and deletion or return of data at the end of the arrangement.

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.

Where Estu is the Data Controller, the Data Protection Lead / DPO will assess whether a personal data breach is notifiable to the ICO and, where required, ensure notification is made without undue delay and normally within 72 hours of Estu becoming aware of the breach. Where Estu is acting as Data Processor, Estu will notify the relevant Data Controller without undue delay and support the Data Controller in meeting its obligations.

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.

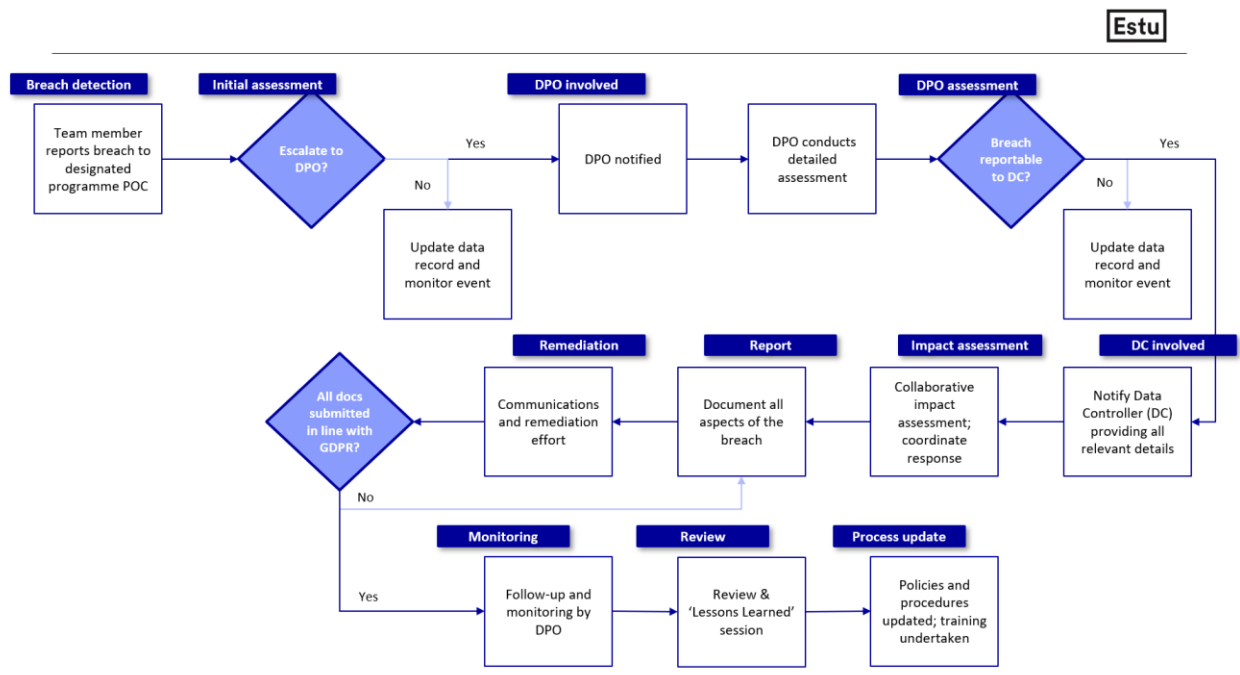
7. Documentation and reporting:

- 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.

Fig. 1 – Estu's data breach notification process, aligned with GDPR requirements



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.

Estu will normally respond to data subject rights requests within one calendar month of receipt. Where a request is complex or multiple requests have been made, this period may be extended where permitted by law, and the individual will be informed.

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.

Where Estu uses AI-enabled tools or automated systems to support business, learning or administrative activities, personal data must only be used where there is a lawful basis, appropriate safeguards are in place, and the tool has been approved for that purpose. Staff must not enter learner, staff, client or other confidential personal data into public or unapproved AI tools.

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 effectively 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): Bruce Storey

Email: bruce.storey@estuglobal.com

Related policies and documents

This policy is to be read in conjunction with other policies and procedures, including those listed below.

Policy Name	Policy Number
Maladministration and malpractice policy	203
Quality assurance policy	204
Whistleblowing policy	108

Reviewed and signed on behalf of Estu's Board: Bruce Storey

Name: Bruce Storey

Role: COO, Estu Global Ltd.

Signing date: 27/02/2026

Date of next review: 26/02/2027