Estu Global Ltd

Information Security Policy

v1.0

Policy version control

Issue	Date	Approved By	Position	Revision Notes
V1	09.06.26	Bruce Storey	COO	New policy
Next Review Date: June 2027			Policy Owner: COO	

Information Security Policy

Contents

Policy Statement

Estu Global Ltd is committed to protecting the confidentiality, integrity and availability of the information, systems and data it uses to deliver training, apprenticeship, employer engagement and business support services.

As an Ofsted-regulated training provider, Estu processes information relating to learners, employers, staff, associates, suppliers and other stakeholders. This includes personal data, learner records, safeguarding-related information, commercial information, funding and compliance evidence, and operational business records.

Estu recognises that effective information security is essential to maintaining learner trust, employer confidence, regulatory compliance and operational resilience. This policy sets out the principles, responsibilities and controls Estu applies to protect its information assets and reduce the risk of unauthorised access, misuse, loss, disruption or compromise.

Estu maintains Cyber Essentials certification and seeks to operate proportionate information security controls aligned to the Cyber Essentials scheme, relevant data protection legislation, contractual obligations and the operational needs of a small but regulated training provider.

Estu outsources IT support and technical management to Lumina Technologies. Estu retains overall accountability for information security governance, while Lumina supports the implementation, management and maintenance of agreed technical controls.

Scope

This policy applies to:

- all Estu employees;
- directors and members of the Senior Leadership Team (SLT);
- associates, contractors and consultants working on behalf of Estu;
- third parties with authorised access to Estu systems or data;
- Estu-owned or Estu-managed devices;

- cloud-based systems and platforms used by Estu;
- personal data, learner data, safeguarding information, commercial records and operational information held by Estu.

This policy applies to all information and systems used to support Estu's operations, including but not limited to:

- Microsoft 365;
- Outlook, Teams, SharePoint and OneDrive;
- Bud (Learning Management System);
- Zoho CRM;
- finance, payroll and compliance systems;
- learner records and portfolio systems;
- company devices and managed endpoints;
- documents, records and files held electronically or in hard copy.

Policy Objectives

The purpose of this policy is to:

- protect Estu's information assets from unauthorised access, disclosure, alteration, loss or destruction;
- support compliance with UK GDPR, the Data Protection Act 2018 and relevant contractual requirements;
- maintain information security controls aligned to Cyber Essentials;
- support continuity of training delivery, learner support and business operations;
- ensure that all staff understand their responsibilities for keeping information secure;

- reduce the risk of phishing, malware, account compromise, data breach and cyber disruption;
- ensure appropriate access controls are applied to learner, employer, safeguarding and business data;
- define clear reporting and escalation routes for suspected security incidents;
- support continuous improvement through training, review and lessons learned.

Information security principles

Estu's approach to information security is based on the following principles:

Confidentiality	Information must only be accessed by people who are authorised and have a legitimate business need to use it.
Integrity	Information must be accurate, complete and protected from unauthorised or accidental alteration.
Availability	Systems and data must be available to authorised users when required to support training delivery, learner support, funding compliance and business operations.
Least privilege	Users should only have the access they need to perform their role. Access should be reviewed and removed when no longer required.
Secure by default	Systems, devices and accounts should be configured securely, with appropriate controls such as multi-factor authentication, malware protection, secure sharing permissions and regular security updates.
Shared responsibility	Information security is the responsibility of all staff, not only the COO, DPO or outsourced IT provider.

Roles and responsibilities

Board

The Board retains ultimate accountability for Estu's governance, operational resilience and risk management. The Board will be informed of significant information security incidents, major data breaches, cyber-attacks or material disruption to Estu's ability to deliver critical services.

Chief Operating Officer

The COO is the owner of this policy and is responsible for:

- overseeing Estu's information security governance;
- ensuring appropriate policies, procedures and controls are in place;
- liaising with Lumina Technologies on outsourced IT and technical controls;
- ensuring information security risks are reviewed and managed proportionately;
- coordinating internal response to significant information security incidents;
- ensuring relevant staff training and awareness activity is undertaken;
- supporting client, funder and regulatory assurance requests relating to information security.

Data Protection Officer

The DPO is responsible for oversight of data protection compliance, including:

- data breach assessment and escalation;
- supporting compliance with UK GDPR and the Data Protection Act 2018;
- advising on data subject rights and lawful processing;
- supporting the COO in reviewing data handling, retention and sharing arrangements;
- ensuring that personal data incidents are managed in line with Estu's Privacy & Data Protection Policy.

Line Managers

Line managers are responsible for:

- ensuring their teams understand and follow this policy;
- ensuring access requests are appropriate for the user's role;
- notifying the COO or Lumina when access needs to change or be removed;
- supporting completion of mandatory information security and data protection training;
- reporting suspected incidents promptly.

All employees, associates and contractors

All users of Estu systems are responsible for:

- keeping passwords and authentication methods secure;
- using multi-factor authentication where required;
- reporting suspected phishing, suspicious emails, security concerns or data breaches immediately;
- only accessing information needed for their role;
- using Estu-approved systems for Estu work;
- handling learner, employer, staff and commercial information responsibly;
- completing mandatory training;
- complying with this policy and related policies.

Lumina Technologies

Lumina Technologies provides outsourced IT support and technical implementation of agreed controls. This may include support with:

- Microsoft 365 administration;
- endpoint and device management;
- user account administration;
- access requests and access removal;
- security updates and patching;

- malware and endpoint protection;
- Microsoft 365 backup arrangements;
- technical incident response;
- security advice and recommendations.

Estu remains accountable for information security governance and decision-making. Lumina is expected to support Estu in maintaining appropriate technical controls and to advise Estu of material security risks, vulnerabilities or recommended improvements.

Cyber Essentials alignment

Estu maintains Cyber Essentials certification and uses the Cyber Essentials control areas as a practical baseline for its information security controls.

The five Cyber Essentials control areas are reflected in Estu's approach as follows:

1. **Firewalls and internet gateways**

   Estu seeks to ensure that internet-facing systems and network connections are appropriately protected and configured to reduce unauthorised access. Where firewall or network controls are managed by Lumina or another supplier, Estu will rely on those suppliers to configure and maintain them in line with agreed security requirements and recognised good practice.

2. **Secure configuration**

   Estu systems and devices should be configured securely. Unnecessary services, unsupported software and insecure default settings should be avoided or removed where identified. Administrative privileges should be restricted to authorised users only.

3. **User access control**

   Access to Estu systems must be based on business need and role requirements. User accounts must be created, amended and removed through agreed processes. Access to sensitive information, including

learner records, safeguarding information and commercial data, must be restricted to authorised users.

4. **Malware protection**

   Devices and systems used for Estu work must have appropriate malware protection in place. Users must not intentionally disable security tools or attempt to bypass security controls.

5. **Security update management**

   Supported software, operating systems and devices should be kept up to date with security patches and updates. Unsupported systems should not be used for Estu business unless a specific risk assessment has been completed and approved.

Access control and authentication

Access to Estu systems is controlled according to user role and business need.

Estu will:

- use individual user accounts wherever possible;
- avoid shared accounts unless there is a clear business need and suitable controls are in place;
- require multi-factor authentication for key business systems where available and appropriate;
- apply role-based access to systems and SharePoint sites;
- restrict administrator access to authorised users only;
- remove or amend access promptly when staff leave or change roles;
- review access permissions periodically;
- maintain appropriate controls over external sharing.

Users must:

- keep passwords confidential;
- not share login credentials;

- not approve multi-factor authentication prompts they did not initiate;
- report unexpected authentication prompts or suspected account compromise immediately;
- use strong passwords or passphrases;
- not reuse Estu passwords for personal accounts or unrelated services.

Joiners, movers and leavers

Estu will operate appropriate processes for staff and associate access.

New starters

Access will be provided based on role requirements. New starters will receive relevant induction covering information security, data protection and acceptable use of Estu systems.

Role changes

Where a user changes role or responsibilities, access should be reviewed and amended to ensure permissions remain appropriate.

Leavers

When an employee, associate or contractor leaves Estu, access to Estu systems should be removed promptly. This includes email, Microsoft 365, SharePoint, Bud, Zoho and any other relevant business systems.

Where required, Estu may retain or transfer business records from the user's account in accordance with operational, legal and data protection requirements.

Device and endpoint security

Users must ensure that devices used for Estu work are kept secure.

Estu will seek to ensure that company-managed devices:

- are protected by appropriate endpoint security tools;
- are kept up to date with security updates;

- use supported operating systems and software;
- are configured securely;
- are protected against unauthorised access;
- can be managed or supported by Lumina where applicable.

Users must:

- keep devices physically secure;
- lock screens when devices are unattended;
- avoid storing Estu information on unmanaged personal devices unless authorised;
- report lost or stolen devices immediately;
- not install unauthorised software on Estu-managed devices;
- not disable malware protection, security updates or management tools.

Where personal devices are used for Estu work, users must take reasonable steps to protect Estu information, including device passcodes, secure storage and use of approved cloud systems rather than local storage wherever possible.

Microsoft 365, SharePoint and cloud systems

Estu uses Microsoft 365, including Outlook, Teams, SharePoint and OneDrive, to support communication, collaboration and document management.

To preserve confidentiality and integrity, Estu uses dedicated SharePoint sites and access controls to manage access to programme, learner, employer and operational information.

Users must:

- store Estu documents in approved locations such as SharePoint or OneDrive;
- avoid storing business documents only on local devices;
- check permissions before sharing files externally;

- avoid sending sensitive personal data by email unless necessary and appropriately protected;
- use approved systems for learner and employer records;
- avoid downloading or exporting personal data unless required for a legitimate business purpose;
- ensure files containing learner, safeguarding or sensitive data are shared only with authorised recipients.

External sharing should be limited to what is necessary and should be reviewed where appropriate. Links should not be set to broad or open access unless there is a clear business need and risk has been considered.

Email security and phishing awareness

Email is a common route for phishing, malware, fraud and account compromise. All users must remain vigilant when using email and collaboration tools.

Users should treat the following as warning signs:

- unexpected document sharing links;
- requests to sign in after clicking an email link;
- unexpected multi-factor authentication prompts;
- urgent requests to make payments or change bank details;
- unusual messages from known contacts;
- attachments or links that are unexpected or unrelated to current work;
- requests for passwords, codes or security information.

Users must not enter passwords into pages reached from suspicious links. If a user is unsure whether a document sharing email is genuine, they should verify using a separate route, such as contacting the sender directly by phone or Teams, or accessing the relevant system directly through a browser rather than clicking the email link.

Users must report suspected phishing promptly to the COO and/or Lumina in accordance with Estu's incident reporting process.

If a user has clicked a suspicious link, entered credentials, approved an unexpected MFA prompt or believes their account may be compromised, they must report this immediately. A rapid response can significantly reduce the impact of an incident.

Data protection and confidentiality

Estu processes personal data relating to learners, staff, employers and other stakeholders. All personal data must be handled in line with Estu's Privacy & Data Protection Policy.

This includes requirements relating to:

- lawful processing;
- data minimisation;
- data accuracy;
- data retention;
- secure sharing;
- data subject rights;
- breach reporting;
- processor and controller responsibilities.

Learner information must only be accessed and used for legitimate Estu purposes, including training delivery, learner support, safeguarding, quality assurance, funding compliance, audit, reporting and administration.

Safeguarding information must be treated as highly confidential and shared only with those who have a legitimate need to know, in line with Estu's Safeguarding & Prevent Policy.

Commercial information, client information, internal financial information and staff records must also be protected from unauthorised access or disclosure.

Backups, recovery and business continuity

Estu recognises that availability of systems and data is essential to maintaining training delivery, learner support, funding compliance and business operations.

Business continuity and recovery arrangements are set out in Estu's Business Continuity Management Framework & Plan. That plan identifies critical business functions, including apprenticeship training delivery, learner safeguarding, funding compliance and ILR submission, payroll and financial operations, data access and digital learning platforms, and employer communication.

Estu's approach includes:

- use of cloud-based systems to support continuity;
- regular backup arrangements for relevant systems and data;
- escalation processes for IT disruption, cyber incidents and data breaches;
- prioritisation of critical business functions;
- recovery objectives for core digital platforms and learner records;
- lessons learned following major incidents or disruptions.

Lumina supports Estu with agreed backup, restoration and Microsoft 365 support arrangements. Estu will periodically review whether backup and recovery arrangements remain appropriate for its operational and contractual requirements.

Supplier and third-party security

Estu works with suppliers and technology providers to deliver its services. Suppliers may include IT support providers, learning platforms, CRM providers, awarding organisations, public funding bodies, consultants and other delivery partners.

Where suppliers process personal data or have access to Estu systems, Estu will seek to ensure that appropriate contractual, technical and organisational safeguards are in place.

Supplier arrangements should consider:

- the nature of the data or system access involved;
- whether personal data is being processed;
- confidentiality requirements;
- access control;
- security obligations;
- incident reporting expectations;
- data retention and deletion;
- business continuity and service availability;
- compliance with relevant legal and contractual requirements.

Lumina Technologies is Estu's outsourced IT support partner. Estu will liaise with Lumina on relevant IT security risks, technical control improvements, incident response and assurance requirements.

Security incident reporting and response

All staff must report actual or suspected information security incidents promptly.

Examples of information security incidents include:

- suspected phishing;
- malware or ransomware;
- lost or stolen devices;
- accidental disclosure of personal data;
- unauthorised access to systems or files;
- suspected account compromise;
- unusual login activity;
- unauthorised forwarding rules or mailbox changes;
- loss of access to critical systems;

- cyber-attack or attempted cyber-attack;
- sharing information with the wrong recipient.

Users must report incidents to the COO, DPO or Lumina as soon as possible. Where the incident involves personal data, Estu's Privacy & Data Protection Policy and data breach process must be followed.

Where an incident materially affects Estu's operations, systems or ability to deliver critical services, Estu's Business Continuity Management Framework & Plan may be invoked.

Following a significant incident, Estu will review what happened, identify lessons learned and update controls, training or procedures where required.

Security awareness and training

All staff are required to understand their information security responsibilities.

Estu will provide or arrange information security awareness activities proportionate to the size and risk profile of the organisation. This includes mandatory annual e-learning for Estu employees covering data protection and phishing awareness.

Training and awareness may include:

- induction training for new starters;
- annual data protection refresher training;
- phishing awareness training;
- reminders following emerging threats or live incidents;
- updates when policies or procedures change;
- targeted guidance for users with access to sensitive data or privileged systems.

Completion of mandatory training will be monitored and followed up where required.

Acceptable use of systems

Estu systems must be used responsibly, lawfully and for legitimate business purposes.

Users must not:

- use Estu systems for unlawful activity;
- access information without authorisation;
- share passwords or authentication codes;
- bypass security controls;
- install unauthorised software;
- store Estu information in unapproved systems without authorisation;
- send confidential or personal data to unauthorised recipients;
- use personal email accounts for Estu business unless expressly authorised;
- copy Estu data to personal storage locations without a legitimate business need;
- deliberately introduce malware or harmful code;
- ignore or conceal suspected security incidents.

Reasonable personal use of systems may be permitted where it does not interfere with work, create security risk, breach law or policy, or damage Estu's reputation.

Remote and hybrid working

Estu supports remote and hybrid working where appropriate. Remote working must be conducted securely.

Users working remotely must:

- use secure internet connections;
- keep devices secure and supervised;

- avoid working with confidential information in public where it may be seen or overheard;
- use approved systems for storing and sharing documents;
- ensure video calls and online sessions are managed appropriately;
- report device loss, theft or suspected compromise immediately.

Remote delivery and online learning must also take account of safeguarding, learner wellbeing and confidentiality requirements.

Records, retention and secure disposal

Information must be retained in accordance with Estu's legal, contractual, funding and operational requirements.

Learner records and funding-related evidence must be retained in line with applicable funding, audit and regulatory requirements. Personal data must not be retained for longer than necessary unless there is a legal, contractual or legitimate business requirement to do so.

When information is no longer required, it must be securely deleted, archived or disposed of in accordance with Estu's data protection procedures.

Hard copy documents containing personal, sensitive or confidential information must be stored securely and disposed of securely when no longer required.

Monitoring and review

Estu may monitor systems, access, activity and security events where necessary to protect systems, investigate incidents, comply with legal or contractual obligations, or maintain operational resilience.

Monitoring will be proportionate and conducted in accordance with applicable law, data protection requirements and contractual obligations.

This policy will be reviewed:

- at least annually;
- following a significant information security incident;

- following major changes to Estu's systems, suppliers or operating model;
- following changes to relevant law, regulation, Cyber Essentials requirements or client obligations.

Updates will be approved by the COO and, where appropriate, reviewed by Lumina Technologies for technical accuracy.

Continuous improvement

Estu is committed to continuous improvement in information security.

This includes:

- reviewing incidents and near misses;
- updating training and awareness activity;
- reviewing supplier and system risks;
- maintaining Cyber Essentials certification;
- reviewing access controls and system permissions;
- responding to emerging threats, including phishing and account compromise;
- improving policies and procedures where required.

Information security improvement actions may be recorded through Estu's operational planning, risk management or governance processes.

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
Business Continuity Management Framework & Plan	102
Safeguarding & Prevent Policy	302
Data Protection Policy	401

Reviewed and signed on behalf of the Board:

By: Bruce Storey, COO

Signing date: 10/06/2026

Date of next review: 01/06/2027