TITLE	REF	VERSION
Information Security and Data Protection Policy	CP019	1

APPROVAL BODY:	DATE	REVIEW DATE
Corporation	20 April 2020	20 April 2021

LEAD PERSON	Director of Governance; Group Director of IT		
EQIA DATE	20 March 2020	DPIA DATE	20 March 2020

INFORMATION SECURITY AND DATA PROTECTION POLICY

Policy Statement

Information security and data protection are critical for a positive and safe environment for our learners and staff, in line with our Learning Philosophy. Activate Learning will protect the security of our IT and data systems to safeguard everyone's privacy and the continuance of our services.

Purpose

This policy outlines our approach to data protection and information security, and our responsibility toward this.

Scope

This policy applies to all information systems, software and physical records, and to all who have access to them. This policy covers all data processing activity, including collection, storage, sharing and deletion.

Responsibilities

As users of Activate Learning's systems, we are all responsible for:

- protecting the information we handle and following relevant policies and processes;
- respecting the boundaries identified in relevant paperwork and guidance; and
- remaining vigilant to data security threats, including cyber-attacks.

Directors, managers and team leaders are responsible for:

- ensuring their teams follow this policy and relevant procedures and guidelines; and
- maintaining their data protection related paperwork.

The IT Team is responsible for:

- maintaining the system-level security of Activate Learning's IT systems;
- monitoring and responding to security threats; and
- providing advice and guidance on the use of IT systems.

The Data Protection Officer is responsible for:

- providing advice, guidance and training about data protection;
- monitoring compliance with relevant guidelines and maintaining central records; and
- coordinating responses to data breaches and data subject rights requests.

Commitment Statement – Data Protection

Data Protection Core Principles

We are committed to the principles of data protection:

- **Lawful, fair and transparent processing:** We only process personal information where:
  - we have a lawful basis to do so;
  - it is considered fair to the subject of the information; and
  - they have been informed about it (usually through Privacy Notices).

- **Purpose limitation and data minimisation:** We are clear about the purpose for collecting personal information and only use it for compatible purposes. We avoid duplication of information by using central

databases and cloud sharing facilities where possible.

- **Accuracy:** We are committed to keeping information accurate and up to date and promptly correcting erroneous data.

- **Storage limitation:** We store information in a secure and orderly way, so that we keep it no longer than is necessary. Departmental Retention Schedules support this.

- **Security, integrity and confidentiality:** See 'Information Security' below.

- **Transfer limitation:** We recognise that some countries may not provide the same standard of data protection. Because of this, we do not transfer information outside the European Economic Area without due care and the approval of the DPO.

- **Data subjects' rights and requests:** We recognise people's data rights, including:
  - the right to request access to data;
  - erasure or rectification of data; or
  - the right to request information about the data we hold about them.

  We all look out for such requests and report them immediately to the DPO. The DPO responds promptly in accordance with the Exercise of Rights Procedure.

- **Privacy by design:** We seek to find creative, efficient and effective solutions that reflect the principles of data protection and information security. All policies and new data processes are subject to a Data Protection Impact Assessment.

Automated Processing and Automated Decision-Making
Before we undertake automated processing or decision-making, we will conduct a Data Protection Impact Assessment and seek the approval of the DPO.

Direct Marketing
We only promote our services in ways that respect people's privacy and comply with the law. As such, our Marketing Team manage any promotional and marketing activity in line with the Direct Marketing Guidelines. We ensure that any direct promotional activity is approved by the Marketing Team.

Freedom of Information
As a public authority, we publish information in line with our Publication Schedule and process requests for information promptly, in line with the Freedom of Information Procedure. We all remain vigilant to requests made under the Freedom of Information Act and report them immediately to the DPO.

Record Keeping
We keep robust departmental and central records of our data processing activities. Where we process information based on consent, we keep records of this.

Training, Audit and Governance
We ensure that we provide access to data protection and information security training, including annual online training. We deploy Data Protection Champions, who receive additional training and provide support and guidance to their teams. We carry out internal audits regularly to identify best practice and areas for improvement. The Data Protection Committee oversees data protection activity and compliance.

Commitment Statement – Information Security

Security, integrity and confidentiality
We make sure that our information and systems are safe from misuse by following IT guidelines. Everyone at Activate Learning should:

- only use secure devices to access Activate Learning information and systems;
- manage passwords and account access securely;
- only use authorised email and cloud storage accounts to access, store, or share information;
- make proper use of secure digital and physical storage solutions;
- share information securely through Office 365; and
- dispose of information securely, such as through the confidential waste facilities provided.

Breaches of data security
We respond quickly and comprehensively to breaches in data security to minimise the impact on the Activate Learning and any people affected. We remain vigilant to potential breaches and report them to the DPO (and the Group Director of IT in the case of IT related breaches) immediately. We handle reported breaches in line with the Data Breach Procedure and report high risk to the Information Commissioner's Office and/or data subjects as appropriate. We may follow up failure to report breaches to ensure staff fully understand the importance of reporting, including disciplinary action where necessary.

Monitoring of IT Systems
We may lawfully monitor electronic communications on Activate Learning systems, including individual mailboxes and files, for the following purposes:
- supporting the operation and security of a system;
- detecting or investigating unauthorised use of systems, suspected misconduct, or criminal activity;
- evidencing transactions;
- quality control, training and/or ensuring the respect and dignity of staff and students;
- checking messages for an absent member of staff;
- monitoring calls to a support line.

References
This Policy complies with the following legislation:
- Data Protection Act 2018
- General Data Protection Regulation 2018
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003

This Policy should be read in conjunction with the following Activate Learning Policies and Procedures:
- Acceptable Use Policy
- Exercise of Rights Procedure
- Data Breach Procedure
- Freedom of Information Procedure
- Departmental Retention Schedules
- Publication Schedule
- Data Protection Impact Assessment Guidelines
- Direct Marketing Guidelines