



IT Policy

Presented by: **Innovate Learning Centre CIC**

Author: ASAD SARWAT
Approved by: SMT
Date: JAN 2026
Next Review Date: JAN 2027

Registered Office: 73 Mellish Road, Walsall, England, WS4 2DG
Contact Address: 78a Walsall Road, Sutton Coldfield, Birmingham, B74 4QY
Phone: 0121 716 7286 | Email: info@innovatelearning.co.uk

1.0 Introduction

1.1 Purpose

This IT Policy outlines the responsibilities, protocols, and safeguards for managing and using information technology systems at Innovate Learning Centre CIC. The policy ensures effective use, protection of data, and alignment with our educational mission.

1.2 Scope

This policy applies to all Innovate staff, learners, contractors, and third-party service providers who access or manage the Centre's digital platforms, networks, or data.

2.0 Acceptable Use of IT Resources

2.1 Academic Use

IT systems should primarily be used to support teaching, learning, research, and administration. Personal use is permitted only if it does not interfere with academic priorities or breach security protocols.

2.2 Prohibited Activities

Users must not engage in unlawful file sharing, unauthorized software installation, cyberbullying, or access of harmful or inappropriate content.

3.0 Learning Platforms and Digital Access

3.1 Moodle & VLE

All coursework, assignments, and communication are to be conducted through Innovate's Moodle Virtual Learning Environment. Users must log in securely and only access content relevant to their role.

3.2 Remote Learning Tools

Approved platforms such as Zoom, Teams, and Google Meet must be used in line with Innovate's online learning and safeguarding protocols.

3.3 Session Security

Systems are configured to automatically log out idle users and enforce secure login credentials to prevent unauthorized access.

4.0 Password and Account Management

4.1 Password Standards

Users must set strong, unique passwords that are regularly updated. Passwords must never be shared or written down in insecure places.

4.2 Multi-Factor Authentication (MFA)

All user accounts require two-factor authentication (2FA) for accessing sensitive systems or learner data.

4.3 Account Monitoring

Inactive or compromised accounts are regularly reviewed and disabled if necessary to prevent breaches.

5.0 Data Protection and Information Security

5.1 Data Confidentiality

All personal and academic data is protected under GDPR and Innovate's Data Protection Policy. Users must not share data outside authorised systems.

5.2 Device Security

All devices accessing Innovate's systems must have antivirus protection, full disk encryption, and secure access settings.

5.3 Encryption & Backups

Sensitive data is encrypted during transmission and backup. Systems are routinely backed up and tested for recovery readiness.

6.0 Roles and Responsibilities

6.1 IT Department

Responsible for managing infrastructure, enforcing technical controls, monitoring systems for misuse, and responding to incidents.

6.2 Academic and Support Staff

Must ensure secure handling of learner data, report issues, and model appropriate use of systems.

6.3 Students

Expected to use IT resources respectfully, report concerns, and follow e-safety guidance provided by staff.

6.4 Data Protection Officer (DPO)

Oversees compliance with GDPR and data protection policies, including audit readiness and response planning.

7.0 Reporting Security Incidents

7.1 Breach Notification

Any suspected data breach, unauthorized access, or loss of device must be reported immediately to the IT Helpdesk and DPO.

7.2 Investigation Process

The IT Department will investigate all incidents promptly, involving external authorities when necessary.

7.3 Disciplinary Measures

Policy violations may result in restricted access, formal warnings, or dismissal, depending on severity.

8.0 Monitoring and Compliance

8.1 Usage Logs

All access to Innovate's IT systems is logged. These logs may be reviewed to ensure policy compliance.

8.2 Random Audits

Unannounced system checks may be performed to assess risk exposure and enforce standards.

8.3 Legal and Regulatory Alignment

All IT activities must align with UK GDPR, Safeguarding regulations, and Innovate's internal frameworks.

9.0 Policy Review

9.1 Review Schedule

This policy is reviewed annually or in response to significant technological or regulatory changes.

9.2 Staff and Learner Awareness

Inductions, refresher training, and reminders ensure that all users understand and adhere to this policy.