IT Security & Acceptable Use Policy

March 2025
Doc Name: **IT Security & Acceptable Use Policy**
Doc Number: ITSAP
Review Date: 03/2026

1: Purpose

This policy establishes the security measures and acceptable use guidelines for CIFA Education Ltd's IT systems. It ensures that IT resources are used responsibly, safeguarding sensitive data and maintaining compliance with UK GDPR. Please refer to our **GDPR Compliance and Data Handling Policy, (Doc Ref: GDPR).**

2: Scope

This policy applies to all employees, contractors and authorised users who access CIFA Education Ltd's IT systems, including:

- Company devices (laptops, mobile phones and storage devices)
- Cloud-based platforms (Digital Ocean, Learning Management Systems www.cifa.ac)
- Communication tools (email, instant messaging, and video conferencing)
- Any system handling personal, financial or confidential data

3: IT Security Measures

3.1: Access Control

- Access to IT systems is granted based on job roles and responsibilities.
- Multi-factor authentication (MFA) is required for all critical systems.
- User accounts must be regularly reviewed and deactivated when no longer needed.

3.2: Data Protection & Encryption

- Personal and financial data must be encrypted during transmission and storage.
- Cloud storage services must use secure authentication and encryption standards.
- Employees must follow CIFA's **GDPR Compliance and Data Handling Policy, (Doc Ref: GDPR)** guidelines for handling and processing personal data.

3.3: Software & System Security

- All software must be kept up to date with the latest security patches.
- Only approved applications may be installed on company devices.
- Antivirus and endpoint protection must be installed on all devices.

3.4: Network Security

- Firewalls and intrusion detection systems are implemented on CIFA networks.
- Public Wi-Fi should not be used to access company systems unless connected via VPN.
- Regular penetration testing is conducted to assess vulnerabilities.

3.5: Incident Response & Reporting

- Any suspected security breach must be reported to the Compliance Officer immediately.
- Data breaches will be handled according to CIFA's **Data Breach Plan and Procedure**, (**Doc Ref: DBPP)**. Employees must cooperate with investigations into IT security incidents.

4: Acceptable Use Guidelines

4.1: Use of Company IT Resources

- IT resources must only be used for business-related activities.
- Users must not share login credentials or allow unauthorised access to company systems.

4.2: Email & Communication Tools

- Business email accounts must not be used for personal communications.
- Suspicious emails must be reported and not opened.
- Employees must follow GDPR-compliant communication practices.

4.3: Internet Usage

- Accessing unauthorised or inappropriate websites is strictly prohibited.
- Downloading unauthorised software or content is not permitted.

4.4: Personal Devices & Remote Work

- Employees must use company-approved devices for handling sensitive data.
- Remote access must be secured using VPNs and strong authentication methods.

5: Responsibilities & Compliance

- All users must comply with this policy to protect CIFA's IT infrastructure.
- The Compliance Officer is responsible for monitoring IT security measures.
- Non-compliance may result in disciplinary action or access restrictions.

6: Policy Review & Updates

- This policy will be reviewed annually or after any major security incident.
- Updates will be communicated to all employees.