Cyber Security Arrangements Policy

Company: Achieve UK Training Ltd
Address: 95 Grove Lane, Handsworth, Birmingham, B21 9HF
Phone: 0121 454 2525
Mobile: 07941015599
Email: contact@achieveuktraining.com
Website: www.achieveuktraining.com
Opening Hours:
Monday – Friday: 10:00 AM – 5:00 PM
Saturday: 10:00 AM – 3:00 PM

Policy Owner: Manav Arora
Approval Date: 01/02/2025
Review Date: December 2027

---

1. Purpose

This policy sets out the cyber security arrangements that Achieve UK Training Ltd has implemented to protect the confidentiality, integrity, and availability of all digital information and systems. It ensures compliance with relevant legislation, including the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

---

2. Scope

This policy applies to all:

- Employees (full-time, part-time, temporary)
- Contractors and consultants
- Volunteers and interns
- Third-party providers and stakeholders accessing the company's data or systems

It covers all digital information, including:

- Client personal data
- Staff records
- Financial and operational data
- Training materials and student coursework
- Communication systems and web services

---

3. Roles and Responsibilities

3.1 Management

- Ensure policy implementation and compliance
- Provide resources for security tools and training
- Approve access levels and vendor contracts

3.2 Staff

- Comply with cyber security practices
- Report any suspected breaches or phishing attempts immediately
- Attend mandatory cyber security training

3.3 IT Support / Administrator

- Maintain and monitor IT infrastructure
- Ensure software updates and patches are applied
- Oversee backup systems and restore processes
- Investigate and respond to cyber incidents

---

4. Access Control

- All user accounts are protected by **strong passwords** (minimum 8 characters, including upper/lowercase, numbers, and symbols)
- Access is granted based on the principle of **least privilege**
- Accounts are reviewed regularly and deactivated when no longer needed
- **Multi-Factor Authentication (MFA)** is enabled on all administrative and remote systems
- Devices must auto-lock after 5–10 minutes of inactivity

---

5. Data Security

5.1 Storage

- Data is stored securely on encrypted local servers or reputable UK-based cloud providers
- Sensitive personal data is encrypted both **in transit** and **at rest**
- Paper records are stored in locked filing cabinets with restricted access

5.2 Backup

- Automated daily backups are conducted and stored offsite or in secure cloud infrastructure
- Backup integrity is tested **monthly**
- Restore procedures are in place and tested **quarterly**

---

6. Email & Internet Usage

- Staff must **not open** unsolicited attachments or click on suspicious links
- Company email is to be used for work-related communication only
- Internet access is monitored and restricted where necessary to prevent access to malicious websites
- Emails containing sensitive data must be encrypted or sent via secure portals

---

7. Device and Network Security

- Antivirus and endpoint protection software is installed and updated automatically
- All devices are protected by firewalls and monitored for unusual activity
- Staff must not connect **unauthorised USB devices** to company equipment
- Public Wi-Fi must be avoided or used only with a secure VPN

---

8. Mobile Device Policy

- Mobile phones and tablets used for work must have passcodes, screen locks, and encryption enabled
- Lost or stolen devices must be reported immediately
- Remote wipe capabilities must be activated on all mobile devices with access to company systems

---

9. Cyber Security Training & Awareness

- All staff undergo **induction cyber security training**
- Annual refresher training includes topics such as:
    - Phishing and social engineering
    - Password best practices
    - Safe data handling
    - Secure remote working
- Monthly cyber awareness bulletins are circulated internally

---

10. Incident Management & Reporting

- Any suspected breach must be reported to the IT Administrator or Manager **within 30 minutes**
- A Cyber Incident Response Plan is in place and includes:
  - Containment of threat
  - Notification to affected parties
  - Root cause analysis
  - Recovery procedures
- Serious incidents are reported to the **Information Commissioner's Office (ICO)** within 72 hours, if applicable

---

11. Remote Working and BYOD (Bring Your Own Device)

- Remote access is permitted only through secure VPN connections
- Personal devices must comply with company security requirements before accessing systems
- Company data must not be stored permanently on personal devices

---

12. Vendor and Third-Party Management

- All third-party vendors must comply with the same cyber security standards
- Data sharing is governed by Data Processing Agreements (DPAs)
- Regular reviews of third-party security compliance are conducted

---

13. Policy Review and Audit

- This policy will be reviewed **annually** or after:
  - A major cyber security incident
  - A significant change in systems or business operations
  - Regulatory or legal changes
- Internal audits are conducted **twice a year** to ensure compliance with this policy

---

14. Related Policies and Documents

- Data Protection Policy
- IT Acceptable Use Policy
- Remote Work Policy

- Cyber Incident Response Plan
- Staff Confidentiality Agreement

For questions or concerns regarding this policy, please contact:
📧 **contact@achieveuktraining.com**
📞 **0121 454 2525 | 07941015599**