Online Safety & E-Security Policy

Achieve UK Training Ltd
Address: 95 Grove Lane, Handsworth, Birmingham, B21 9HF
Phone: 0121 454 2525 | **Mobile:** 07941 015599
Email: contact@achieveuktraining.com
Website: www.achieveuktraining.com

---

1. Policy Statement

Achieve UK Training Ltd is committed to providing a safe, inclusive, and respectful online learning and working environment for all staff, learners, and stakeholders. This policy outlines our approach to managing and mitigating risks associated with digital learning platforms, online communication, cyberbullying, harassment, and data protection.

---

2. Scope of the Policy

This policy applies to:

- All staff, tutors, and contractors working for or on behalf of Achieve UK Training Ltd.
- All learners enrolled in our programmes.
- All platforms and technologies used for communication, collaboration, learning, and assessment.
- Any activity involving the internet or digital devices, whether conducted onsite or remotely.

---

3. Responsibilities

3.1 Organisation Responsibilities

- Maintain secure systems with appropriate antivirus, firewalls, and encryption.
- Ensure compliance with UK GDPR and Data Protection Act 2018.
- Provide training and guidance on online safety and cyber awareness.
- Monitor use of company platforms to detect and respond to abuse.

3.2 Staff Responsibilities

- Promote a culture of digital respect and safety.
- Report incidents of cyberbullying, harassment, or e-security breaches.
- Use work accounts responsibly and protect login credentials.

- Follow all e-safety protocols and participate in regular training.

3.3 Learner Responsibilities

- Respect others when communicating online.
- Avoid sharing personal or sensitive information on public forums.
- Report inappropriate behaviour, threats, or harassment.
- Use provided systems for learning purposes only.

---

4. Cyberbullying

4.1 Definition

Cyberbullying is any form of bullying that occurs through electronic means such as social media, emails, messaging apps, or learning platforms.

4.2 Examples

- Sending abusive or threatening messages
- Posting false or malicious content online
- Impersonating others to cause harm
- Excluding individuals from digital groups or discussions

4.3 Preventative Measures

- Clear codes of conduct and online etiquette guidelines
- Regular digital citizenship education for learners
- Prompt removal of abusive content when reported

4.4 Reporting and Action

- Victims or witnesses should report incidents to the course tutor or designated safeguarding officer.
- Reports will be investigated confidentially and sensitively.
- Disciplinary action, which may include suspension or removal from programmes, will be taken where necessary.

---

5. Online Harassment

5.1 Definition

Online harassment involves any repeated, unwanted contact or communication that causes distress or fear, including discriminatory or sexual harassment.

5.2 Forms of Harassment

- Inappropriate or sexualised messages or images
- Racist, sexist, homophobic, or otherwise discriminatory language
- Persistent messaging after being asked to stop

5.3 Consequences

- Any instance of harassment will result in immediate investigation.
- Serious or repeated violations may be referred to legal authorities.
- Support will be provided to victims, including access to counselling or pastoral care if needed.

---

6. E-Security & Data Protection

6.1 System Security

- All users must use secure passwords and log out of shared devices.
- Devices must be locked when unattended.
- Files containing personal data must be encrypted or stored in secure, password-protected systems.

6.2 Phishing & Online Scams

- Staff and learners should be cautious of suspicious emails and links.
- The organisation will never request passwords or bank details via email.
- Suspected phishing attempts must be reported immediately.

6.3 Use of Personal Devices (BYOD)

- Personal devices must have antivirus software installed.
- Users are responsible for ensuring that their device is secure when accessing work or learning platforms.

---

7. Risks of Working Online

7.1 Key Risks

- **Data leakage** due to weak passwords or poor storage practices
- **Phishing scams** targeting emails or social engineering attacks
- **Mental health challenges** from screen fatigue or isolation
- **Distractions and productivity issues** in home environments

7.2 Mitigation

- Regular breaks, ergonomic workstations, and well-being check-ins
- Use of productivity tools and scheduled work hours
- Access to IT support for troubleshooting or security concerns

---

8. Reporting Procedures

All incidents must be reported to the designated safeguarding officer or through:

📧 **Email:** contact@achieveuktraining.com
📞 **Phone:** 0121 454 2525 or 07941 015599

Reports will be acknowledged within 2 working days and investigated promptly. Outcomes and support plans will be shared with all involved parties.

---

9. Policy Review

This policy will be reviewed annually or earlier if required by changes in legislation, technology, or operational practices. The next review date is scheduled for **April 2026**.

---

10. Related Policies

- Safeguarding Policy
- Equality & Diversity Policy
- Learner Code of Conduct
- Data Protection & GDPR Policy

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