The Ace Academy

IT and E-Safety Policy

1. Policy Statement

The Ace Academy is committed to ensuring that all students, staff, and stakeholders use technology safely, responsibly, and effectively. This policy outlines our approach to managing IT systems, safeguarding users online, and promoting digital literacy across all settings, including outreach and 1:1 mentoring.

Filtering and Monitoring to Keep Learners Safe
At The ACE Academy, we use robust filtering and monitoring systems to ensure that all online activity within our provision is safe and appropriate. Our network is protected by industry-standard web filters that block harmful, illegal, or inappropriate content, including extremist material and sites that pose safeguarding risks. These measures are regularly reviewed and updated to comply with statutory guidance and best practice standards. Staff are trained to respond promptly to alerts, and any breaches are investigated in line with our safeguarding procedures. Parents are encouraged to support safe online practices at home, reinforcing our shared commitment to digital safety.

2. Aims

- To protect students and staff from online risks and harm.
- To promote responsible and ethical use of technology.
- To ensure secure and appropriate use of IT systems and digital devices.
- To educate students about digital safety, privacy, and cyberbullying.
- To comply with relevant legislation and safeguarding guidance.

3. Scope

This policy applies to:

- All students, staff, volunteers, and contractors
- All devices and platforms used for educational purposes
- All settings, including:
    - Partner schools
    - Community venues
    - Outreach and home-based sessions
    - Online and remote learning environments

4. Legal and Regulatory Framework

This policy is informed by:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Education Act 2011
- Keeping Children Safe in Education (KCSIE)
- Prevent Duty Guidance
- The Children's Online Privacy Protection Act (COPPA)

---

5. Acceptable Use of Technology

For Students

- Use devices and internet access only for educational purposes.
- Respect others online and avoid sharing harmful or inappropriate content.
- Do not share personal information or passwords.
- Report any online concerns or incidents to a trusted adult or mentor.

For Staff

- Use work devices and accounts for professional purposes only.
- Ensure all student data is stored securely and shared appropriately.
- Monitor student use of technology during sessions.
- Model safe and respectful online behaviour.

---

6. Device and Internet Use

- Devices used for outreach must be encrypted and password-protected.
- Public Wi-Fi should be avoided unless secured with a VPN.
- Students may use their own devices only with staff supervision and consent.
- All internet activity may be monitored for safeguarding purposes.

---

7. Online Safety Education

- E-safety is embedded in mentoring and PSHE sessions.
- Topics include:
    - Cyberbullying and online abuse

    - Digital footprints and privacy
    - Social media safety
    - Sexting and online grooming
    - Reporting and blocking harmful content

---

8. Cyberbullying and Online Abuse

- All incidents of cyberbullying will be taken seriously and investigated.
- Victims will be supported through mentoring and safeguarding referrals.
- Perpetrators will be subject to behaviour interventions and possible sanctions.
- Serious incidents may be reported to the police or external agencies.

---

9. Remote and Online Learning

- Online sessions must be conducted via approved platforms.
- Staff must ensure sessions are secure, private, and recorded where appropriate.
- Students must be dressed appropriately and in a suitable environment.
- Parents/carers should be informed of online session times and expectations.

---

10. Data Protection and Privacy

- All personal data must be stored in line with our Data Protection Policy.
- Staff must not store student data on personal devices.
- Emails and digital communications must be professional and secure.
- Students must be taught about their rights to privacy and data protection.

---

11. Reporting and Responding to Incidents

- All e-safety concerns must be reported to the Designated Safeguarding Lead (DSL).
- Incidents are recorded on CPOMS or the designated safeguarding system.
- Where necessary, external agencies (e.g., CEOP, police) will be contacted.
- Parents/carers will be informed of serious incidents involving their child.

---

12. Staff Training

- All staff receive annual training on IT security and e-safety.

- Training includes:
    - Recognising online risks
    - Responding to disclosures
    - Using digital tools safely
    - Preventing radicalisation and online grooming

13. Monitoring and Review

- IT systems and usage are monitored regularly by the SLT and IT Lead.
- This policy is reviewed annually or following a significant incident or change in guidance.
- Feedback from staff and students informs updates to the policy.

14. Related Policies

- Safeguarding and Child Protection Policy
- Data Protection Policy
- Behaviour and Wellbeing Policy
- Remote Learning Policy
- Anti-Bullying Policy

15. Contact Information

For concerns or questions about IT or e-safety, contact:

Aaron Shelton - Designated Safeguarding Lead (DSL)
The Ace Academy
☎ Phone07305829143
📧 Email: ashelton@theaceacademy.co.uk