QMX ACADEMY

IT AND E-SAFETY POLICY

Last Updated

19th June, 2025

Contents Page

1. Policy Statement

QMX Academy is committed to promoting the safe, secure, and responsible use of digital technology. We aim to protect learners and staff from online harm while fostering positive digital citizenship across all areas of academy life.

2. Purpose and Scope

This policy outlines expectations, procedures, and safeguarding practices related to the use of technology at QMX Academy. It ensures compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Keeping Children Safe in Education (KCSIE)
- Prevent Duty
- Children and Social Work Act 2017

This applies to:

- All students in Key Stages 3 and 4
- All staff, contractors, and visitors using academy devices, systems, or internet access

3. Acceptable Use of IT Systems

- All users must sign an Acceptable Use Agreement before accessing IT systems.
- Use of devices must support educational and professional activities only.
- Sharing passwords or accessing unauthorised content is strictly prohibited.

4. Digital Safeguarding and E-Safety

- Staff are trained to identify online safeguarding risks including grooming, radicalisation, and exploitation.
- Age-appropriate filters and monitoring tools are in place to protect users from harmful content.
- Students receive regular education on staying safe online.

5. Monitoring and Filtering

- Web filtering software blocks access to harmful, explicit, or non-educational content.
- Internet use is monitored to ensure compliance with safeguarding and acceptable use policies.
- IT staff may audit user activity in response to safeguarding or security concerns.

6. Cyberbullying and Online Conduct

- All instances of cyberbullying are treated seriously and managed in line with the Behaviour and Anti-Bullying Policies.
- Students must treat peers with respect in all digital communications.
- Misuse of platforms or online harassment may lead to disciplinary action.

7. Use of Personal Devices (BYOD)

- Students are not permitted to use personal mobile phones during learning hours unless authorised for educational use.
- Staff must follow the academy's code of conduct when using personal devices on-site.

8. Data Security and Password Protection

- All users must:
    - Use secure, unique passwords and update them regularly.
    - Log out of shared devices after use.
    - Report any data breaches immediately.
- Staff handling personal data must complete data protection training.

9. Social Media Guidance

- Students are educated on the responsible use of social media.
- Staff must not connect with students via personal social media accounts.
- Reputational damage caused by inappropriate online behaviour will be addressed as a disciplinary matter.

10. Roles and Responsibilities

- **Director/SLT**: Ensure systems and policies are in place to support safe IT usage.
- **DSL**: Monitor online risks and manage safeguarding incidents.
- **IT Coordinator**: Maintain filtering, security systems, and compliance.
- **All Staff**: Promote safe digital practices and report concerns.
- **Students**: Use technology responsibly and report any online safety concerns.

11. Reporting Concerns and Breaches

- Concerns must be reported to the Designated Safeguarding Lead (DSL) or IT lead immediately.
- All incidents will be logged and, where necessary, escalated to appropriate authorities.

12. Training and Awareness

- All staff complete annual e-safety training.
- Students engage in termly digital safety lessons appropriate to their age and key stage.
- Parents are provided with guidance and resources for supporting online safety at home.

13. Policy Review

This policy is reviewed annually, or earlier if required due to significant changes in technology, legislation, or incidents.