# Mazahirul Uloom London E-Safety Policy

## 1. Policy Statement

At MUL, we are committed to ensuring that all students and staff use digital technologies safely and responsibly. The purpose of this policy is to:  
- Protect students and staff from online harm.  
- Promote responsible and respectful use of digital technology.  
- Support the curriculum through safe use of digital tools.  
- Meet statutory safeguarding requirements, including the Prevent Duty and Keeping Children Safe in Education (KCSIE).

## 2. Scope

This policy applies to all members of the school community who have access to the school’s IT systems, including students, staff, governors, visitors, and volunteers, whether accessing on-site or remotely.

## 3. Roles and Responsibilities

* Headteacher:

Ensures e-safety is embedded in the school’s safeguarding strategy. Provides resources for training and technology.

* Designated Safeguarding Lead (DSL):

Leads on e-safety incidents and ensures appropriate responses. Liaises with parents/carers and external agencies where necessary.

* IT Manager/Technician:

Implements filtering and monitoring systems. Maintains the security of school networks and systems.

* Staff:

Model appropriate online behaviour. Report any e-safety concerns to the DSL immediately. Teach students how to stay safe online.

* Students:

Use digital devices and the internet responsibly. Report any concerns, bullying, or inappropriate content. Follow the Acceptable Use Policy (AUP).

* Parents/Carers:

Support the school’s e-safety approach at home. Monitor their child’s online behaviour. Engage with school-led online safety workshops.

## 4. Education and Training

• E-safety is embedded in PSHE, ICT, and across the curriculum.  
• Staff receive annual training, including on the latest risks such as online grooming, radicalisation, and cyberbullying.  
• Workshops and newsletters are provided to parents/carers.

## 5. Technical Measures

• Internet filtering and monitoring provided by [e.g. Smoothwall/NetSupport/Impero].  
• Email and web activity monitored for inappropriate content.  
• User access is password-protected with age-appropriate permissions.

## 6. Use of Mobile Devices and Personal Technology

• Students must not use personal phones or smart-watches in the school.  
• Staff use of personal devices must comply with safeguarding and GDPR expectations.  
• Taking photos or videos of students is only allowed using school equipment and with consent.

## 7. Social Media and Online Communication

• Staff must not accept students as 'friends' or communicate with them via personal social media accounts.  
• Students are taught to use social media responsibly and understand privacy settings.  
• The school will respond to online bullying or reputational damage involving students or staff.

## 8. Responding to Incidents

All incidents, including cyberbullying, sexting, or exposure to harmful content, must be reported to the DSL. The school will follow procedures outlined in:  
- The Safeguarding and Child Protection Policy  
- DfE guidance including Searching, Screening and Confiscation (2022)  
- Local authority safeguarding protocols

## 9. Data Protection and Privacy

• The school adheres to UK GDPR and the Data Protection Act 2018.  
• Digital records are stored securely and access is limited.  
• Consent is obtained for use of student data, photos, and online tools.

## 10. Policy Review

This policy will be reviewed annually or in response to significant changes in technology, legislation, or guidance.

## Appendices (Attached below)

A: Student Acceptable Use Policy  
B: Staff Acceptable Use Policy  
C: E-Safety Incident Report Form  
D: Useful Links and Resources (e.g. CEOP, NSPCC, ThinkUKnow)

**Date Reviewed: July 2025**

**Next Review Due: June 2026**

**Policy Lead: Khalil Goddard Headteacher & Designated Safeguarding Lead (DSL)**

**Approved by: Governing body.**

**E-Safety Policy Appendices**

**Appendix A: Student Acceptable Use Policy (AUP)**

As a student at [School Name], I agree to:  
- Use school technology for educational purposes only.  
- Never share personal information online, including passwords, addresses, or phone numbers.  
- Be respectful to others when communicating online.  
- Report anything that makes me feel unsafe or uncomfortable to a teacher or trusted adult.  
- Not attempt to bypass the school’s internet filtering system.  
- Never download, install, or use software without permission.  
- Only access content that is appropriate and safe.  
- Understand that my internet and device usage may be monitored.

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix B: Staff Acceptable Use Policy (AUP)**

As a member of staff at [School Name], I agree to:  
- Use school ICT systems and internet services responsibly and professionally.  
- Not share personal information or communicate with students via personal social media accounts.  
- Report any safeguarding concerns related to online activity to the DSL.  
- Use school devices for school-related tasks, following data protection guidelines.  
- Keep all passwords secure and never share them.  
- Not install or use unauthorised software or hardware.  
- Ensure any digital communication with students is appropriate and school-related.  
- Be aware that school systems are monitored for safety and security.

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

Staff Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix C: E-Safety Incident Report Form**

Date of Incident: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Time of Incident: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Reported By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name(s) of Student(s) Involved: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Details of the Incident:

Actions Taken:

Referred to (e.g. DSL, Headteacher): \_\_\_\_\_\_\_\_\_\_\_\_

Follow-Up/Outcome:

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_

**Appendix D: Useful Links and Resources**

- CEOP (Child Exploitation and Online Protection): https://www.ceop.police.uk/  
- NSPCC Online Safety: https://www.nspcc.org.uk/keeping-children-safe/online-safety/  
- ThinkUKnow: https://www.thinkuknow.co.uk/  
- UK Safer Internet Centre: https://www.saferinternet.org.uk/  
- Childnet: https://www.childnet.com/