



London Academy E-safety Policy

#We are the Future

Approved By:	Emily Olot
Position:	Director
signed:	
Date:	March 2025
Proposed Review Date:	August 2026
Review Team:	Head of schools



London Private Academy E-safety Policy

Vision:



Mission Statement:

Empowering children with 21st-century skills.

Providing a happy, safe, and caring environment for all individuals.

Promoting learning through project-based and technology-based tools.

Delivering an exciting curriculum while fostering high self-esteem and respect.

Partnering with parents to develop children educationally, morally, spiritually, physically and socially.



1. Rationale and Technical Context

This Digital Wellbeing and E-Safety Policy is essential for ensuring that all members of the London Academy community—students, staff, and parents—understand their responsibilities regarding the safe, responsible, and healthy use of digital technology. Our goal is to foster confident digital citizens while mitigating online risks and maintaining a protected learning environment.

Technical Control Environment

London Academy operates a dedicated 1:1 digital learning environment designed for safety and focus:

- **Device Standardisation:** All students utilise a Samsung tablet for educational purposes.
 - **Mobile Device Management (MDM):** These devices are centrally managed via MDM software. This system is critical to maintaining a safe learning environment.
 - **App and Website Restriction:** The MDM software actively restricts the use of applications and web browsing to a list of school-approved websites and educational apps only. This prevents access to non-educational or potentially harmful online content.
 - **Misuse Protocol:** Any misuse, circumvention, or deliberate attempt to bypass the MDM restrictions or inappropriate behaviour online is considered a serious breach of school rules and will be addressed strictly under the Behaviour for Learning Policy.
-

2. Aims of the Digital Wellbeing and E-Safety Policy

- **Student Protection:** To protect students from digital harm, including access to inappropriate content, cyberbullying, and contact from harmful third parties.
- **Responsible Citizenship:** To educate students on the principles of responsible digital citizenship, including data privacy, copyright, and ethical online behaviour.
- **Wellbeing Promotion:** To promote healthy habits concerning screen time, digital footprint management, and the balance between digital and physical activities.
- **Enforcement and Compliance:** To ensure all network and device usage complies with the school's technical control measures (MDM) and the sanctions outlined in the Behaviour for Learning Policy.

3. Key Terminology

Term	Definition at London Academy
E-Safety	Protecting users from harm and risk on the internet, encompassing online security, digital privacy, and addressing cyberbullying.
Digital Wellbeing	The impact of technology use on a user's physical, mental, and social health, focusing on balance and control.
MDM	Mobile Device Management: The software used by the school to configure, secure, and restrict functionality on the school-owned Samsung tablets.
Digital Footprint	The trail of data left by a person's activities on the Internet (e.g., posts, files, records of website visits).



Cyberbullying	Bullying that takes place using digital technology, including social media, messaging apps, and online gaming platforms.
---------------	--



4. Implementation and Curriculum Integration

E-Safety and Digital Wellbeing are integrated into the curriculum and school operations across all Key Stages to ensure continuous awareness.

Key Stage	Years	Implementation Strategy
Primary (KS1 & KS2)	Years 1–6	Foundational Digital Skills: Taught through computing lessons and PSHE time. Focus includes understanding safe search engines, knowing what personal information not to share, and reporting concerns to an adult (known as "Tell"). All learning takes place on MDM-secured devices.
Key Stage 3 (KS3)	Years 7–9	Digital Citizenship and Responsibility: Focus on the impact of a digital footprint, identifying fake news and phishing, managing online identities, and responsible use of online communication tools (within MDM limits). Content is often delivered in Form Time and IT/Computing lessons.
Key Stage 4 & 5 (KS4 & KS5)	Years 10–13	Advanced Awareness and Preparation: Focus on the legal and ethical implications of online behaviour, intellectual property, career management of an online presence, and preparing for independent, unsupervised online access post-school. Content is integrated into PSHE, Business, and IT subjects.



5. Staff and Parental Roles

Staff Responsibilities

All staff must model excellent digital citizenship and adhere to the Staff Code of Conduct concerning technology use. They are required to report any misuse of devices or instances of cyberbullying to the Senior Leadership Team immediately, following established safeguarding procedures.

Parental Partnership

Parents are expected to support the school's E-Safety policy by:

- Reinforcing the importance of responsible online behaviour at home.
 - Monitoring their child's technology use outside of school hours, recognizing that the MDM restrictions may be less restrictive off the school network.
 - Reporting any online activity that causes concern or distress to the school.
-



6. Policy Review

This Digital Wellbeing and E-Safety Policy will be reviewed annually by the Safeguarding Committee, the Senior Leadership Team, and the Director. The review will account for changes in educational technology (including updates to MDM and device policies), emerging online threats, and compliance with best international E-Safety practice and Moroccan law.