Online Safety and Acceptable Use Policy

Bromley Technical School (BTS)

1. Statement of Intent

Bromley Technical School provides access to a range of technologies, including the internet, computer networks, and mobile devices, to enhance learning and prepare pupils for a technology-driven world. We recognise the vital importance of technology in education, but prioritize the safety and well-being of our pupils when using these resources.

This policy sets out the expectations for acceptable use of all school IT facilities and addresses the necessary procedures to ensure the online safety of the entire school community, in compliance with the *Independent School Standards Regulations*, the *Education Act 2011*, and *Keeping Children Safe in Education* guidance.

2. Scope

This policy applies to all users of school IT systems: pupils, staff, volunteers, contractors, and visitors. It covers all school-provided devices, network access, and the use of personal devices while connected to the school environment.

3. Acceptable Use Agreement (AUA) for Pupils

Pupils are required to sign an Acceptable Use Agreement (AUA) upon admission. Unacceptable use of technology will be treated as a breach of the school's Behaviour Policy and may result in sanctions.

Pupils must **not**:

- Access, upload, download, or distribute obscene, inappropriate, illegal, defamatory, or harmful materials.
- Bypass or attempt to bypass the school's internet filtering systems or security measures.
- Share passwords or use another person's login credentials.
- Engage in any form of cyberbullying, harassment, or intimidation of others.
- Use the school network for personal commercial activities or illegal purposes.
- Install software or hardware without explicit permission from the IT department.
- Bring in USB sticks or external media without scanning it for viruses first.

Pupils **must**:

- Use technology ethically and responsibly, showing respect for others online.
- Report any concerns about online safety, inappropriate content, or cyberbullying to a staff member immediately.
- Adhere to copyright laws and respect intellectual property rights.

4. E-Safety Procedures and Safeguards

4.1 Internet Access and Filtering

The school uses a robust internet filtering system designed to block access to inappropriate or harmful content, in line with DfE requirements. While no filter is perfect, we actively monitor internet usage. Any attempts to access blocked content are logged and reviewed by the IT Manager and DSL team.

4.2 Monitoring and Privacy

Users should be aware that the school monitors all activity on the school network and school devices, including email communications and internet usage logs. Monitoring is conducted to ensure compliance with this policy and to safeguard pupils. Users should have no expectation of privacy when using school systems.

4.3 Social Media

- **Pupils** should use social media responsibly and respectfully. They must not use social media during lessons or on school grounds in a way that disrupts the learning environment or breaches the Anti-Bullying Policy.
- **Staff** are prohibited from connecting with pupils on personal social media accounts. All professional communication must take place via official school communication channels.

4.4 Data Protection

All data handling must comply with the UK Data Protection Act and GDPR. The school ensures pupil and staff personal data is securely stored and transmitted.

5. Review

This policy will be reviewed annually by the IT Manager, the Headteacher, and the Governors, or in response to new technologies or changes in statutory guidance.

Policy Last Reviewed: December 2025 **Next Review Date:** December 2026