



ONLINE SAFETY POLICY

Reviewed September 2026

Next Review: September 2027

1. Policy Overview

This policy outlines Little Ilford School's commitment to ensuring all students, staff, and visitors use digital technologies safely, responsibly, and ethically. It covers access to school hardware, personal devices on school grounds, and digital interactions connected to the school community.

2. Key Roles & Responsibilities

Role	Key Responsibilities
Governing Body	• Hold the Headteacher to account for overall policy implementation and monitoring. • Ensure all staff receive initial and annual online safety training, including filtering and monitoring expectations. • Ensure students are taught online safety, tailored for vulnerable groups, abuse victims, and SEND students. • Review and ensure appropriate filtering and monitoring systems meet DfE standards annually. • Ensure regular staff meetings are coordinated into the long term plan and review DSL online safety logs.

Headteacher	• Ensure staff understand the policy and implement it consistently throughout the school. • Ensure regular training takes place for every member of staff and that monitoring records are checked and updated where necessary.
Designated Safeguarding Lead (DSL)	• Lead operational responsibility for online safety and review the policy annually with the Headteacher and Governors. • Oversee, understand, and work with the Network Manager on filtering and monitoring systems. • Manage, log, and report all online safety and cyberbullying incidents; liaise with external agencies as needed. • Conduct annual risk assessments, deliver staff updates/training, and report regularly to the Headteacher and Governors.
Network Manager and ICT Infrastructure team (Dataspire)	• Implement, update, and review filtering, monitoring, virus, and malware security systems (including monthly security checks). • Block access to dangerous sites/files and prevent access to harmful, inappropriate, or extremist content • Log and address online safety and cyberbullying incidents in line with school policies. • Liaise with the Senior Leadership Team member with ICT oversight. • Maintains age-appropriate web filtering (e.g., Smoothwall, Lightspeed), ensures network security, and conducts routine logs/audits.
All Staff & Volunteers	• Understand, sign, and consistently implement the policy and Acceptable Use Agreement (linked document). • Ensure students follow their Acceptable Use Agreement (linked document). • Report filtering/monitoring failures via CPOMs and request system bypasses through the Network Manager for education. • Log all online safety or cyberbullying incidents with the DSL; maintain an 'it could happen here' attitude toward sexual violence/harassment, radicalisation, bullying, grooming and online abuse.

Parents & Carers	• Contact the school with any queries or concerns regarding the policy. • Ensure their child reads, understands, and agrees to the student Acceptable Use Agreement (Linked document). • Access external guidance resources (e.g., UK Safer Internet Centre, Childnet International) for home support.
-----------------------------	--

3. Infrastructure, Filtering & Monitoring

- **Web Filtering:** The school employs filtering systems that meet The London Borough of Newham's statutory standards to block access to harmful content, including illegal content, radicalisation risks, self-harm materials, and adult content.
- **Network Logging:** User activity on school devices and guest networks is logged. Attempting to bypass filters using VPNs or proxies is strictly prohibited and leads to disciplinary action.
- **School Hardware:** All school-issued devices (tablets, laptops) are subject to monitoring software, regardless of whether they are used on-site or at home.

4. Student Code of Conduct (Acceptable Use)

4.1 Personal Mobile Devices

- Students may bring mobile phones to travel to and from school but they **must** be handed into the year team during morning line ups, kept switched off and out of sight in bags during school hours (08:30–15:15). Students found in possession of a mobile device during the school day will have the device confiscated until the end of the week, or for longer periods of time if there is persistent misuse or failure to adhere to the policy.
- From 2025, students beginning in year 7 must not bring smartphones and may only bring 'brick' phones to school. The same rules above apply to these devices.
- Unauthorised recording, photography, or filming of students or staff is strictly forbidden.

4.2 Cyberbullying & Online Behavior

- Bullying, harassment, or intimidation carried out online (whether on or off school grounds) will be treated with the same severity as physical bullying.
- Creating fake social media profiles or posting content that damages the reputation of staff, students,

or the school is a major breach of discipline and will be sanctioned accordingly.

4.3 Data Privacy & Passwords

- Students must never share passwords or access another individual's account.
- Personal identifiable information (phone numbers, addresses) must never be shared on public or school platforms.
- Staff should never leave a computer unlocked and unattended. Failure to do so may result in disciplinary action.
- Staff should not display confidential professional information in view of students on SIMS, Satchel, Century or any other platforms. Seating plans should be confidential

5. Safeguarding & Reporting Incidents

Any online safety incident must be handled in accordance with the school's Safeguarding and Child Protection Policy.

1. **Immediate Intervention & Assessment:** (*Priority: Ensure immediate safety*) The member of staff who identifies or receives the report must ensure the student is safe. If necessary, secure any digital evidence (e.g., taking screenshots) without copying or transmitting illegal content (such as explicit images).
2. **Logging the Incident:** (*Mandatory escalation*) Log the concern on CPOMS within 2 hours, notifying the DSL or DDSL, Safeguarding team and relevant Head of Year via email alongside the entry.
3. **DSL Assessment & Sanctions:** (*Action stage*) The DSL determines appropriate next steps: applying school disciplinary sanctions, contacting parents, or referring to external services (e.g., Internet Watch Foundation, local police, Children's Social Care).
4. **Review & Support:** (*Follow-up care*) Provide targeted pastoral support for affected students and update filtering/network configurations if a technical breach occurred.

6. Curriculum & Training

- **Student Education:** Online safety is delivered through PSHE/RSE lessons, ICT classes, and regular assemblies. Key focus areas include cyberbullying, image-sharing risks (e.g., 'sexting'), online grooming, digital footprint, and fake news.
- **Staff Training:** All staff receive mandatory e-safety training during induction and annual safeguarding updates to keep pace with emerging online trends and risks

7. GDPR Compliance

Online Safety Policy: GDPR & Data Protection Compliance

This section outlines how the school complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 across all e-safety procedures, digital learning, and network monitoring systems.

1. Core Principles of Data Protection in Online Safety

- **Data Minimisation & Purpose Limitation:** The school processes personal data only for legitimate, statutory safeguarding and educational purposes. Safeguarding logs, network tracking, and incident reports capture only the necessary data needed to ensure child safety.
- **Lawful Basis for Processing:** Processing student data for monitoring and safeguarding is conducted under the lawful bases of *Public Task* (fulfilling statutory obligations under Keeping Children Safe in Education) and *Vital Interests* (protecting children from harm).
- **Data Security & Encryption:** All personal data—including sensitive safeguarding logs stored on platforms like CPOMS—must be encrypted in transit and at rest. Personal data must never be stored on unencrypted USB drives or personal devices.

2. Practical Measures for GDPR Compliance

Compliance Domain	Requirements & Action Plan
Filtering, Monitoring & Privacy	• Staff and students are informed via Privacy Notices and Acceptable Use Agreements (AUAs) that network usage and school-owned devices are subject to filtering and monitoring. • Monitoring logs are treated as confidential, accessible only to authorised personnel (e.g., DSL, Headteacher, IT system administrators).
Personal Data & Media Consent	• Explicit, written parental/carer consent is managed separately for publishing pupil photos, video footage, or work on public or social channels. • Parents sign home-school agreements for use of student information at the beginning of every academic year. • Staff must use school-issued hardware for official photography or recording and must never use personal mobile phones or cameras.
Secure Communication & Storage	• All professional digital communication regarding students must be sent using official school email accounts. • Staff must lock screens when stepping away from workstations and avoid displaying confidential information in public view. • When a child emails a teacher from an unrecognised LIS account, the teacher reports to Little Ilford Safeguarding

	and responds as per SG protocol.
Generative AI & EdTech Usage	• EdTech platforms and third-party tools must undergo Data Protection Impact Assessments (DPIAs) before deployment • Staff and students are prohibited from entering personally identifiable pupil or staff information into unvetted or third-party Generative AI tools. • Teachers using generative AI platforms in school must only use the agreed platform- Google Gemini. Staff should be logged into Gemini through their @littleilford.org account and through the RM portal. For more information on the acceptable use of generative AI, please visit the school's AI policy
Data Breach Management	• Any accidental exposure, loss, or unauthorised access of personal data (e.g., sending an email containing sensitive information to the wrong recipient) must be reported to the Data Protection Officer (DPO) immediately. • High-risk data breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours of discovery.

3. Data Subject Rights & Retention

- **Subject Access Requests (SARs):** students and parents/carers have the right to request access to personal data held by the school. However, safeguarding logs or monitoring reports may be redacted if releasing them would cause serious harm to a child or disclose third-party personal data.
- **Data Retention:** Safeguarding and online safety logs are retained strictly in accordance with statutory retention schedules (e.g., Information and Records Management Society guidelines) and securely deleted once the mandatory holding period expires.

4. Further Link Documents/Policies:

[KCSIE 2026](#)

[HB AI Policy](#)

[HB Acceptable ICT Use Agreement](#)

[HB Curriculum, Assessment and Teaching Policy.docx](#)

[HB GDPR Policy](#)

[HB Home Learning Policy](#)

 HB Privacy Notice Policy (Students)

 HB Students' mobile phone use during educational visits AGREEMENT.docx