



Acceptable Use Agreement

Reviewed by Governors: September 2026

Next review: September 2027

1. Introduction and aims

Information and communications technology (ICT) is vital to teaching and learning, pastoral care and administration at Little Ilford School.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents/carers and governors.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policies on data protection, online safety and safeguarding.
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems.
- Support the school in teaching students safe and effective internet and ICT use.

Scope

This policy covers all users of our school's ICT facilities, including governors, staff, students, volunteers, contractors, visitors, and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can damage our school and our reputation. Breaches of this policy may be dealt with under our [Staff Code of Conduct](#) and will result in disciplinary action by the Governing Body and [Behaviour for Learning Policy](#) for students.

2. Relevant legislation and guidance

This policy aligns with the following legislation and guidance:

- [Data Protection Act 2018](#)
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Data \(Use and Access\) Act 2025](#)
- [Computer Misuse Act 1990](#)
- [Human Rights Act 1998](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- [Education Act 2011](#)
- [Freedom of Information Act 2000](#)
- [Education and Inspections Act 2006](#)

- [Keeping Children Safe in Education 2026](#)
- [Searching, screening and confiscation: advice for schools 2022](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- [Education and Training \(Welfare of Children\) Act 2021](#)
- [Meeting digital and technology standards in schools and colleges](#)

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service.
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, students, volunteers, contractors and visitors.
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

4. Unacceptable use and exemptions

Unacceptable use

Users must not use school ICT facilities (or personal devices, where relevant) to breach the school's policies or procedures. This includes:

- **Illegal and harmful activity:** Access, create, store or share unlawful, discriminatory, defamatory, obscene, pornographic or extremist material.
- **Safeguarding and harassment:** Cyberbully, harass others, or share nude/semi-nude images or livestreams.
- **Social Media:** Communicate online using internet chat rooms, post on message boards, blogs or other social media sites without permission from the Headteacher.
- **Defamation:** Engaging in any activity which defames or disparages the school, or risks bring the school into disrepute.
- **Data and IP breaches:** Infringe copyright, disclose confidential school and/or student data, or cause unauthorised data access.
- **Security:** Bypass filtering and monitoring (e.g. using VPNs, proxies or incognito mode), connect unauthorised hardware, install unapproved software or attempt to gain unauthorised access to the school's ICT facilities.

- **Network and ICT infrastructure:** Connecting any device to the school's ICT network without permission and causing intentional damage (vandalism) to the school's ICT facilities including uploading or the creation of computer viruses.
- **Commercial and financial misuse:** Engage in online gambling, phishing, financial scams or commercial business promotion.

The use of Artificial Intelligence (AI) is covered in the [Use of Artificial Intelligence \(AI\) policy](#). The list above is not an exhaustive list. The school reserves the right to amend this list at any time.

Exemptions

If an otherwise restricted activity is required for legitimate curriculum or administrative purposes (e.g. unblocking a site for research):

- Submit a request via the IT Helpdesk (Dataspire)
- Seek written approval from the School Business Manager

Sanctions

Misuse may result in restricted or revoked ICT access, internal disciplinary measures in line with the [Staff Code of Conduct](#), or referral to external agencies/Police where illegal activity is suspected.

5. Staff (including governors, volunteers, and contractors)

Access to school ICT facilities, account security and passwords

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. **Only school mobile phones or school ipads/tablets and school cameras should be used for the filming or the taking of photos of students.**

Staff must:

- Use equipment and devices for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality.
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device.

- Update software, operating systems and applications when prompted, or as directed by the Network Manager.
- Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks.
- Loss, theft or damage must be reported immediately to the Network Manager, DSL (where appropriate) and School Business Manager.
- Staff passwords must be a minimum of **12 characters** (including uppercase, lowercase, numbers and symbols) and should change regularly. Passwords must remain confidential and must never be reused across multiple services. Accounts must be locked when devices are left unattended.

Access permissions are managed by the Network Manager and IT department. Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Network Manager.

Communication Protocols - use of phones and emails

Staff must use their school email address (@littleilford.org) and school provided phones for all official communications. Personal email addresses or mobile numbers must never be given to students or parents.

Work emails can be used as official records in Freedom of Information (FOI) and Subject Access Requests (SARs). Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. **All email messages should be treated as potentially retrievable.**

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Staff must take extra care when sending sensitive or confidential information by email. If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Business Manager immediately and follow guidance outlined in the [GDPR Policy](#).

School social media accounts

The school has an official Instagram and LinkedIn accounts, managed by the Communication Officer. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the accounts.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the accounts must make sure they abide by these guidelines at all times.

Personal use and devices

Staff are permitted to occasionally use school ICT facilities for personal use, subject to the conditions set out below:

- Does not take place during contact time (teaching hours, non-break time)
- Does not constitute 'unacceptable use' as defined in section 4.
- Takes place when no students are present.
- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes.

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that the use of the school's ICT facilities for personal use falls within the scope of the school's ICT monitoring activities (see the monitoring and filtering section). Where breaches of this policy are found, disciplinary action may be taken.

Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Mobile Phone Policy (section 4 of the [Staff Code of Conduct](#)).

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media ([Staff Code of Conduct](#)) and use of email (see above) to protect themselves online and avoid compromising their professional integrity.

Remote access

Staff can access school materials remotely via Google Workspace (@littleilford.org) and web-based applications (such as RM Unify/Satchel, and SIMS Next Gen where authorised). Direct remote access to local network drives (N: drive) or SIMS .net requires an authorised, Remote Access connection managed by the IT Department and available through the school website. Remote access requires prior written approval from the School Business Manager.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions such as preventing viruses or unauthorised access.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our [GDPR Policy](#).

6. Monitoring and filtering

To comply with Department for Education (DfE) guidance on [meeting digital and technology standards](#), and to safeguard and promote the welfare of children, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Web filtering is managed via LGfL SchoolProtect across all school devices and networks. The IT Department may inspect logs or emails to ensure compliance with this policy. If you come across inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) report this to the Designated Safeguarding Lead (DSL) and the School Business Manager.

The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including for the following purposes:

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy.
- To find lost messages or retrieve messages lost due to computer failure.
- To help in the investigation of alleged wrongdoing.
- To comply with any legal obligation.

The list above is not exhaustive.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
- For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and Business Manager, as appropriate.

7. Students

Access to ICT facilities

Students must only access ICT facilities (workstations, chrome books, Google Classroom and other educational software as well as network locations) under staff supervision and for educational purposes only.

Students must not share their passwords with others, or use their email account to share or download files, including software from the Internet or inappropriate content.

The school may apply sanctions under the [Behaviour for Learning Policy](#) for any digital misuse, either on site or off site. Any safeguarding concerns arising from a student's use of ICT should be logged on CPOMS and reported to the DSL in line with our [Child Protection and Safeguarding Policy](#).

Examples of misuse include, but are not limited to:

- **Illegal and harmful activity:** Access, create, store or share unlawful, discriminatory, defamatory, obscene, pornographic or extremist material. This includes the sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting) and includes images created using generative AI. See the [Use of Artificial Intelligence \(AI\) policy](#) for more guidance on the use of AI.
- **Cyberbullying and harassment:** Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination. This includes the use of inappropriate or offensive language when communicating online.
- **Defamation:** Engaging in any activity which defames or disparages the school, or risks bring the school into disrepute.
- **Data and IP breaches:** Infringe copyright, disclose confidential school and/or student data, or cause unauthorised data access.
- **Security:** Bypass filtering and monitoring (e.g. using VPNs, proxies or incognito mode), connect unauthorised hardware, install unapproved software or attempt to gain unauthorised access to the school's ICT facilities.
- **Network and ICT infrastructure:** Connecting any device to the school's ICT network without permission and causing intentional damage (vandalism) to the school's ICT facilities including uploading or the creation of computer viruses.

8. Parents

We believe it is important to model for students, and help them learn how to communicate respectfully with, and about, others online. Parents/carers play a vital role in helping model

this behaviour for their children, especially when communicating with the school through our website and social media channels.

Parents/carers do not have access to the school's ICT facilities unless they are working for, or with, the school in an official capacity (for instance, as a volunteer). Permission to use the school's facilities will only be granted by the Headteacher. Where parents/carers are granted access in this way, they must abide by this policy.

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the Business Manager or Network Manager.

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer)
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

9. Data Security and Cyber Security

Data security and cyber threats

Please see the glossary (appendix 4) to help you understand cyber security terminology.

All of the school's ICT devices that support software updates, security updates and anti-virus products, will have these installed, and be configured to perform such updates regularly or automatically.

The school makes sure that its devices and systems have an appropriate level of encryption. School staff should be cautious about using personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as student information) out of school. School staff should follow guidelines about data protection outlined in the school's [GDPR Policy](#).

Users should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources without authorisation from the Network Manager.

To meet the Department for Education's guidance on [digital and technology standards in schools and colleges](#) the school use the following to maintain security:

- Firewalls, anti-malware and automated software patch installation
- Off-site and cloud based daily backups of critical systems e.g. SIMS
- User authentication and multi-factor authentication for secure applications e.g. CPOMS
- Annual training for all users, including staff, students and governors about data security, including:
 - o The methods hackers use for tricking people into disclosing personal information, including phishing (also known as social engineering).
 - o Online safety and password security including multi-factor authentication.

- o The physical security of devices, for example not leaving a laptop unlocked and unattended and the risks of using removable storage media, such as USBs
- o How and when to report a cyber attack or data breach.
- Develop, review and test an incident response plan (as outlined in the [Business Continuity & Critical Incident Plan](#) and [Cyber Response Plan](#)) that sets out how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud and the Local Authority of the incident.
- Conduct a cyber risk plan at least annually.
- The school will also check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the [Cyber Essentials](#).

The school will put controls in place that are proportionate, multi-layered, up to date and regularly reviewed and tested. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Data protection

All personal data must be processed and stored in line with data protection regulations and the school's [GDPR Policy](#).

10. Monitoring and review

The headteacher and Business Manager will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year. This policy will be reviewed annually by the Headteacher, School Business Manager, and the Governing Board.

11. Linked policies and procedures

This policy should be read alongside the school's policies on:

- [Online Safety Policy](#)
- [Child Protection and Safeguarding Policy](#)
- [Behaviour for Learning Policy](#)
- [Staff Code of Conduct](#)
- [GDPR Policy](#)
- [Business Continuity & Critical Incident Plan](#)
- [Home Learning Policy](#)

- [Use of Artificial Intelligence \(AI\) policy](#)
- [Cyber Response Plan](#)

Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carers:	
Name of child:	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels and platforms: • Our official Instagram account. • MyEd app, emails and text for parents (for school announcements and information). • Satchel to share information about praise, behaviour points and detentions. • Go4Schools to share information about students' progress and attainment.	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times. • Be respectful of other parents/carers and children. • Direct any concerns or complaints through the school's official channels, so they can be dealt with in line with the school's complaints procedure. I will not: • Use private groups or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way. • Use private groups or personal social media to complain about, or try to resolve, a school-related behaviour issue involving other students. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident. • Upload or share photos or videos on social media, AI or the internet of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	Date:

Appendix 2: Acceptable use agreement for students

Acceptable use of the school's ICT facilities and internet: agreement for students and parents/carers

Name of student:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites, social networking sites or chat rooms.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Use any inappropriate language when communicating online, including Google Classroom.
- Publish information about yourself or others online.
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video.
- Share my password with others or log in to the school's network using someone else's details.
- Use a device to bully another student inside or outside of school.
- Use AI tools and generative chatbots (such as ChatGPT or Google Gemini):
 - To impersonate, bully or harass another person.
 - Generate (including digitally altering) or share explicit or offensive content
 - Input offensive, discriminatory or inappropriate content as a prompt
 - During assessments, including internal and external assessments, and coursework
 - To present AI-generated text or imagery as my own work (you must reference your use of AI and not infringe copyright law.

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (student):

Date:

Parent/carers agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carers):

Date:

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access any illegal or inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
- Use them in any way which could harm the school's reputation.
- Access social networking sites or chat rooms.
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
- Share my password with others or log in to the school's network using someone else's details.
- Share confidential information about the school, its students or staff, or other members of the community.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote any private business, unless that business is directly related to the school.
- Use any unapproved AI tools. Approved AI tools include Google Gemini and Brisk.
- Share identifiable information (unless strictly necessary and only in Google Gemini using your school account).
- Use information provided by AI without acknowledgement of its use and without fact-checking.

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the Designated Safeguarding Lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. Many of these terms are from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove viruses and other kinds of malicious software.
Breach	When your data, computer systems or networks are accessed or affected without authorisation.
Cloud	An on-demand, massively scalable service, hosted on a shared infrastructure where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Any event that threatens the confidentiality, integrity, or availability of data within your computer network, or where the security of your system or service has otherwise been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from unauthorised theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone who uses their technology skills to gain unauthorised access to computers, systems and networks.
Malware	Malicious software. Any kind of software that can damage computer systems, networks or devices, which includes viruses, trojans or any code or content that is harmful.

TERM	DEFINITION
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses with the end aim of fixing them.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails or text messages sent to many people asking for sensitive information (such as bank details or passwords) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
Social engineering	Manipulating people into giving information or carrying out specific actions that's of use to an attacker.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly-targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.