



St. Lawrence Church of England
Primary School

ACCEPTABLE USE OF ICT POLICY

SEPTEMBER 2026

Policy Leader and Computing Lead: James Davis

Headteacher and Designated Safeguarding Lead: Richard Crook

Data Protection Officer: James Davis

Safeguarding Governor: Dotun Fasanya

Last reviewed on: September 2026

Approved by: Governing Body

Next review on: September 2027

CONTENTS

1. Context and Purpose
2. Scope and Status
3. Principles and Responsibilities
4. Accounts Passwords and Access
5. Devices Networks and Physical Security
6. Internet Email and Communications
7. Software Cloud Services and Artificial Intelligence
8. Information Data and Copyright
9. Prohibited and Restricted Use
10. Reporting Incidents and Concerns
11. Monitoring Privacy and Consequences
12. Training Review and Agreement
13. Appendix A Staff Acceptable Use Agreement
14. Appendix B KS2 Pupil Acceptable Use Agreement
15. Appendix C EYFS and KS1 Family Agreement
16. Appendix D Visitor Volunteer and Temporary Staff Agreement

1. CONTEXT AND PURPOSE

The Bible tells us that we are all “children of God” (John 1:12). As part of our school family, everyone who uses school technology is expected to act with integrity, kindness, responsibility and respect. Digital technology supports teaching, learning, safeguarding, communication and the effective running of the school. Safe and responsible use protects children, colleagues, information and the continuity of education.

This policy defines what users may and may not do when using the school’s ICT, networks, accounts, data and digital services. It provides the governing framework for the shorter agreements in the appendices, which users sign or acknowledge in a form appropriate to their role and age.

This policy works with, rather than replaces, the Online Safety Policy, Child Protection and Safeguarding Policy, Data Protection Policy, Artificial Intelligence Policy, Mobile Phones and Smart Devices Policy, Behaviour and Relationships Policy and Staff Code of Conduct.

2. SCOPE AND STATUS

This policy applies to staff, governors, pupils, volunteers, trainee teachers, placement students, agency and supply staff, contractors, visitors, community users and any other person given access to school ICT, networks, Wi-Fi, accounts, data or digital services. It applies to school-owned and school-managed equipment wherever it is used, and to personal equipment used to access school systems or carry out school business.

Access is provided for authorised educational, safeguarding, administrative and professional purposes. Limited incidental personal use by staff may be permitted where it is lawful, reasonable, does not interfere with work, create cost or risk, breach another policy, or involve prohibited content. Where personal use involves mobile phones or smart devices, users must also comply with the requirements of the Mobile Phones and Smart Devices Policy. There is no entitlement to personal use.

Access is conditional on compliance with this policy. A user who cannot or will not agree to the applicable rules may have access withheld or restricted. Safeguarding concerns and staff allegations will always be handled through the correct safeguarding or employment procedure, not merely as an ICT breach.

3. PRINCIPLES AND RESPONSIBILITIES

- **Authorised use.** Use only the accounts, devices, services, data and permissions provided for your role or learning.
- **Safeguarding first.** Report anything that may place a child or adult at risk immediately; do not investigate it yourself.
- **Least access.** Access only information needed for the task and do not use another person's account or privileges.
- **Privacy and security.** Protect personal, confidential and special category data and follow the school's security controls.
- **Professional conduct.** Communicate respectfully and maintain appropriate boundaries and a professional digital footprint.
- **Accuracy and integrity.** Check information, identify sources, respect copyright and never misrepresent work or evidence.
- **Prompt reporting.** Mistakes, suspicious activity, lost equipment, harmful content and control failures must be reported quickly. Prompt, honest reporting helps the school contain harm.

Responsibilities

<u>Role</u>	<u>Responsibility</u>
Governing Body	Approve the policy and receive assurance about implementation, cyber awareness, risks and serious incidents.
Headteacher and senior leaders	Ensure proportionate controls, training, enforcement and coordination between safeguarding, data protection, curriculum and technical support.
Computing or digital lead	Coordinate the policy, user agreements and cyber-awareness activity with technical support, the DSL and DPO.
DSL	Ensure rules and training support safeguarding and lead responses where a child may be at risk.
DPO	Advise on lawful processing, privacy, breaches, DPIAs and data-protection training.
Technical support	Maintain access controls and security; approve or install technology; assist with incidents and evidence; report safeguarding concerns to the DSL.
All users	Understand and follow the rules, protect access and data, and report concerns promptly.

4. ACCOUNTS PASSWORDS AND ACCESS

- use your own named account and never allow another person to use it; shared accounts may be used only where formally authorised and controlled
- keep passwords and authentication codes secret; never ask pupils to share passwords with other pupils
- use a strong, unique password or passphrase and do not reuse a school password for personal services
- use multi-factor authentication where the school requires it or the service provides it for a protected account
- lock the screen or sign out whenever a device is left unattended; do not leave an authenticated device available to pupils or visitors
- never approve an unexpected authentication request; report repeated prompts or suspected compromise immediately
- do not attempt to access accounts, files, systems or administrative functions beyond your permission
- tell technical support promptly when access is incorrect, no longer required or should be removed following a role change or departure.

Passwords should be changed immediately if compromise is suspected or instructed by technical support. The school will not require arbitrary frequent changes unless a system, risk assessment or incident makes this necessary. Passwords must not be written in an insecure place or stored in an unapproved browser or application.

5. DEVICES NETWORKS AND PHYSICAL SECURITY

- handle school equipment carefully, keep it secure and report loss, theft or damage immediately
- use only approved devices and connection methods; personal devices may connect only through an authorised guest or managed arrangement
- do not use personal hotspots, VPNs, proxies or other methods to bypass filtering, monitoring or network controls
- do not disable security settings, firewalls, anti-malware, updates, monitoring, device management or encryption
- do not alter hardware, connect unauthorised equipment or attempt repairs unless authorised
- keep devices away from unauthorised users and from avoidable damage; school devices must not be left visible in unattended vehicles
- use public Wi-Fi only in line with school instructions and with appropriate secure access
- USB storage and other removable media are prohibited by default. They may be used only for an approved specific need and must be supplied or checked by the school and scanned before use
- printing and storage should be limited to what is necessary; confidential printouts must be collected promptly and disposed of securely.

Pupil mobile phones, smart watches, smart glasses and similar personal technology are governed by the Mobile Phones and Smart Devices Policy. Personal devices must never be used by staff or visitors to photograph, record or store pupil information.

6. INTERNET EMAIL AND COMMUNICATIONS

- use the internet for authorised learning, professional or school business and comply with filtering and monitoring arrangements
- use approved school email, messaging, learning and collaboration systems for school communications; staff must not communicate with pupils through personal accounts
- check recipients, permissions, links and attachments before sending; use blind copy where appropriate and do not expose contact details unnecessarily
- do not open unexpected links, attachments or QR codes or respond to requests for passwords, payments or urgent confidential action without verification
- treat unusual requests from senior staff, suppliers, parents or colleagues as potential impersonation or social engineering and verify them using a separate trusted route
- do not send offensive, discriminatory, threatening, sexual, defamatory, misleading or confidential material
- do not create automatic forwarding from school email to a personal account
- report spam, phishing, misdirected communications, inappropriate contact and harmful content using the agreed route.

Official social-media accounts require Headteacher approval and named administrators. Personal social-media use must maintain professional boundaries and comply with the Staff Code of Conduct and Online Safety Policy. Users must not present personal opinions as those of the school.

7. SOFTWARE CLOUD SERVICES AND ARTIFICIAL INTELLIGENCE

- install or use only software, apps, extensions, websites and cloud services approved through the school's process
- do not create school accounts using personal email addresses or agree to contracts, subscriptions or processing terms without authority
- check age restrictions and do not direct pupils to create accounts where the service is not approved for their age or use
- do not circumvent licensing, subscription, copyright or access controls
- use only approved AI tools for school purposes and follow the Artificial Intelligence Policy, AI register, risk assessment and any DPIA requirements
- never enter safeguarding records, confidential information, special category data, identifiable pupil data or unpublished assessment material into a public or unapproved AI tool
- check AI output for accuracy, bias, appropriateness, copyright, privacy and safeguarding risk; professional responsibility remains with the user
- do not use AI to impersonate, deceive, harass, monitor covertly, create sexualised content, produce deepfakes or make a significant decision about a person without authorised human oversight.

A new service or significant change must be considered for safeguarding, privacy, security, accessibility, educational value, age suitability, contract and technical compatibility before use. Convenience or a free account does not remove this requirement.

8. INFORMATION DATA AND COPYRIGHT

- access, use and share personal or confidential information only where authorised and necessary
- store school information only in approved locations and do not copy it to personal email, personal cloud storage, unapproved apps or personal removable media
- use secure sharing permissions and review access before sending a link; "anyone with the link" must not be used for confidential information
- do not download or retain more personal data than needed; follow school retention and secure-deletion arrangements
- work privately when viewing sensitive information and take care that screens, conversations and printouts cannot be seen or heard by unauthorised people
- respect copyright, licences and intellectual property; acknowledge sources and use material within permitted terms
- do not plagiarise or submit AI-generated or copied work as your own; permitted assistance must be acknowledged as directed
- report any loss, unauthorised disclosure, misdirection, unusual access or other possible personal-data breach immediately to the DPO.

9. PROHIBITED AND RESTRICTED USE

Users must not knowingly use school ICT to create, access, store, search for, transmit or promote:

- child sexual abuse material or any sexualised image of a child, including AI-generated or altered imagery
- pornographic, extremist, terrorist, hateful, discriminatory, violent or otherwise illegal material
- bullying, harassment, threats, coercion, grooming, exploitation, impersonation or deliberate humiliation
- content encouraging suicide, self-harm, eating disorders or other serious harm, except within an approved, risk-assessed educational or safeguarding activity
- malware, hacking tools, stolen credentials, methods to evade controls or instructions for unauthorised access
- gambling, unauthorised financial activity, cryptocurrency mining, private business or personal commercial gain
- material that breaches confidentiality, data protection, copyright, licensing or examination rules.

Accidental access must be reported immediately. Do not continue searching, close or minimise the content if safe, and do not copy, screenshot, print, save or forward suspected illegal or indecent material. Approved safeguarding, curriculum, technical or investigative activity may require access to sensitive material; this must be specifically authorised, risk assessed and carried out through the agreed procedure.

10. REPORTING INCIDENTS AND CONCERNS

<u>Concern</u>	<u>Report immediately to</u>
A child may be at risk; grooming, bullying, sexual content, exploitation, self-harm, extremism or other safeguarding concern	DSL or deputy DSL and the school safeguarding system. Emergency services first if there is immediate danger.
Concern about an adult working with children	Headteacher; Chair of Governors if the concern is about the Headteacher.
Lost device, malware, phishing, compromised account, suspicious access or cyber incident	Technical support and the nominated senior leader.
Personal-data loss, unauthorised disclosure or misdirected information	DPO under the Data Protection Policy.
Accidental harmful content, failure of filtering or an attempt to bypass controls	DSL or relevant senior leader and technical support.
Inappropriate pupil use without an evident safeguarding concern	Class teacher or senior leader under the Behaviour and Relationships Policy.

Users must give a factual account and preserve relevant information without conducting their own investigation. Devices or messages that may contain evidence should not be altered unnecessarily. Suspected indecent imagery must not be viewed, copied or forwarded. Technical support may isolate equipment or preserve logs when instructed, but safeguarding decisions remain with the DSL.

11. MONITORING PRIVACY AND CONSEQUENCES

The school filters and monitors use of its networks, services and school-managed devices for safeguarding, security, conduct, system management and legal compliance. Users should not expect personal privacy when using school systems, but monitoring will be necessary, proportionate, transparent and limited to legitimate purposes. Access to monitoring information will be restricted to authorised people.

The school may examine logs, accounts, communications, files or devices where there is a lawful and proportionate reason. It will not routinely monitor private personal accounts. Monitoring and investigations will comply with the Online Safety Policy, Data Protection Policy and applicable staff or pupil procedures.

A response may include education, restorative work, parental contact, restriction or withdrawal of access, a behaviour sanction, safeguarding support or referral, data-protection or cyber response, staff disciplinary action, recovery of costs where lawful, or referral to police or another authority. The response will consider intent, impact, repetition, age, understanding, SEND, vulnerability, professional role and prompt self-reporting.

12. TRAINING REVIEW AND AGREEMENT

Cyber-security and acceptable-use awareness will be included in induction and refreshed at least annually for staff and pupils, and for at least one current governor. Supply, agency, volunteer and other users with logins will receive proportionate information and training as soon as feasible. Training will cover phishing, passwords, multi-factor authentication, device security, removable media, online safety, data protection and incident reporting.

The policy will be reviewed annually and after a serious incident, material technology change or significant change in guidance. The Headteacher, computing or digital lead, technical support, DSL and DPO will contribute, and the Governing Body will approve it.

Staff and regular users will sign or electronically acknowledge the applicable agreement on appointment and at least annually. Pupil agreements will be taught and revisited at the start of each academic year. Agreement supports understanding but does not remove the duty to comply where a signature has not yet been obtained.

13. APPENDIX A - STAFF ACCEPTABLE USE AGREEMENT

I understand that school ICT, accounts, data and services are provided for authorised professional purposes. I agree that I will:

- use only my own authorised account and protect my password and multi-factor authentication
- lock or sign out of devices when unattended and keep school equipment secure
- use approved school systems for school communications and information
- check recipients, links, attachments and sharing permissions
- use only approved software, cloud services, AI tools and storage locations
- never enter pupil, safeguarding or confidential data into an unapproved service or public AI tool
- maintain professional boundaries and never use a personal device to photograph or record pupils
- not bypass filtering, monitoring, security, licensing or access controls
- not connect unauthorised devices or use removable storage unless specifically approved
- report safeguarding concerns to the DSL immediately and report cyber incidents, data breaches, lost equipment, phishing, harmful content and mistakes without delay
- not investigate safeguarding material or view, copy, save, print or forward suspected illegal or indecent imagery
- accept proportionate filtering and monitoring of school systems and cooperate with authorised investigations.

I have read and understood the Acceptable Use of ICT Policy and the related policies relevant to my role. I understand that misuse may lead to restricted access, safeguarding action, disciplinary procedures or external referral.

Name: _____	Role: _____
Signature: _____	Date: _____

14. APPENDIX B - KS2 PUPIL ACCEPTABLE USE AGREEMENT

School technology helps me learn, create and communicate. I agree that:

- I will use my own account and keep my password private
- I will use devices, websites, apps and AI tools only when a member of staff says I may
- I will be kind and respectful and will not send, create or share anything hurtful, frightening, discriminatory or inappropriate
- I will not try to get around filters, monitoring, passwords or security settings
- I will not share personal information, photographs, location or contact details unless a trusted adult at school has approved it
- I will check information and remember that online and AI-generated content can be wrong or misleading
- I will respect other people's work, say where information came from and follow instructions about using AI
- I will handle equipment carefully and tell an adult about damage, loss or anything unusual
- I will tell a trusted adult straight away if something worries or upsets me, if someone contacts me inappropriately, or if I make a mistake
- I understand that the school filters and monitors its systems to help keep people safe.

I understand that adults will help me put things right. Deliberate or repeated misuse may mean that my access is restricted and may be dealt with under the school's behaviour or safeguarding procedures.

Pupil name: _____	Class: _____
Pupil signature: _____	Date: _____
Parent or carer signature: _____	Date: _____

15. APPENDIX C - EYFS AND KS1 FAMILY AGREEMENT

Adults will teach and remind children about these rules in language they understand.

- I use school devices when a grown-up says I can.
- I ask before I click, take a picture or share something.
- I am kind when I use technology.
- I keep my name, password and personal information private.
- I tell a trusted grown-up if I see something strange, upsetting or worrying.
- I look after the equipment and tell an adult if something goes wrong.

Parent or carer agreement: I have discussed these rules with my child. I will support the school's online-safety and acceptable-use expectations and will contact the school if I have a concern.

Child's name: _____	Class: _____
Parent or carer: _____	Date: _____

16. APPENDIX D - VISITOR VOLUNTEER AND TEMPORARY STAFF AGREEMENT

This agreement applies to visitors, volunteers, contractors, agency staff, supply staff and other temporary users who receive access to school ICT, Wi-Fi, accounts or data.

- I will use access only for the authorised purpose and will not share credentials or allow another person to use my access.
- I will use only the network, device and services the school authorises and will not bypass security, filtering or monitoring.
- I will not access, photograph, record, copy or remove pupil or confidential information unless expressly authorised for my role.
- I will not install software, connect equipment or use removable storage without approval.
- I will report any safeguarding concern immediately to the DSL and any technical, security, privacy or data concern to my school contact.
- I understand that school systems may be filtered and monitored and that access may be withdrawn.
- I will return equipment, badges and access credentials and will retain no school information when my work ends.

Name: _____	Organisation or role: _____
School contact: _____	Access required: _____
Signature: _____	Date: _____