



Acceptable Use of Technology Policy

2026/27

This policy sets out expectations for the safe, lawful, ethical and responsible use of technology by pupils, staff, governors, volunteers, contractors, visitors and parents/carers. It forms part of the school's wider safeguarding framework and should be read alongside the Child Protection and Safeguarding Policy, Common Sense Code (Staff Code of Conduct), Behaviour Policy, Data Protection Policy, Mobile Phone/Smart Technology expectations and Online Safety arrangements.

School	Wouldham All Saints Church of England Primary School
Headteacher / DSL	Mrs Victoria Baldwin
Approved by	Governing Board
Review cycle	At least annually and sooner following significant changes to legislation, guidance, technology or safeguarding risk
Policy year	September 2026 – August 2027



1. Introduction and aims

Technology is integral to teaching, learning, communication and school administration. It also creates safeguarding, privacy, data protection, cyber-security and professional-boundary risks. This policy establishes clear expectations so technology can be used positively while protecting children, adults, information and school systems.

- support safe, kind, lawful and responsible use of technology;
- protect pupils from illegal, inappropriate and harmful content and contact;
- set clear expectations for school-provided and personal devices, accounts, networks and online services;
- support effective filtering and monitoring as part of safeguarding;
- protect personal and confidential information and reduce cyber-security risk;
- set clear expectations for artificial intelligence (AI), images, recordings, social media and digital communication;
- ensure age- and ability-appropriate expectations, including reasonable adjustments for pupils with SEND;
- provide clear routes for reporting concerns, incidents and breaches.

The DSL has a key role in the development and review of this policy, supported by senior leaders, the school's IT providers, Data Protection Officer (DPO) and governors. Evidence that relevant groups have received and understood the AUP will be retained through signed/electronic acknowledgements, induction and training records and pupil/parent communication as appropriate.

2. Relevant legislation and guidance

This policy reflects the LESAS Acceptable Use Policies template for 2026/27 and should be read in the context of current statutory and non-statutory guidance, including:

- Keeping Children Safe in Education 2026 (KCSIE);
- Early Years Foundation Stage statutory framework 2026, including safeguarding expectations for mobile phones, cameras and electronic devices with imaging/sharing capabilities and the requirement to have regard to screen use;
- Data Protection Act 2018 and UK GDPR;
- Computer Misuse Act 1990;
- Human Rights Act 1998;
- Education Act 2011 and current DfE Searching, Screening and Confiscation guidance;
- Education and Inspections Act 2006;
- Freedom of Information Act 2000;
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;
- DfE Mobile phones in schools guidance;
- DfE Meeting digital and technology standards in schools and colleges, including filtering and monitoring and cyber-security standards;
- UKCIS guidance on sharing nudes and semi-nudes;
- DfE guidance and support materials on generative artificial intelligence in education and data protection;
- NCSC cyber-security guidance for schools.

National policy and legislation concerning children's access to social media and online services continues to develop. Proposed changes will not be presented as current legal requirements unless and until they are in force.



3. Scope and definitions

This policy applies to all users of school technology and to use both on and off site where school systems, accounts, devices or information are involved, or where personal technology use is linked to a person's role and could affect safeguarding, confidentiality, professional boundaries, school operations or the school's reputation.

- Technology/ICT facilities: networks, Wi-Fi, desktops, laptops, tablets, phones, smart/wearable technology, cameras, software, cloud services, websites, apps, communication platforms, AI tools and any future equivalent service.
- School-provided/approved systems: equipment, accounts, software, platforms and services supplied or formally approved by the school.
- Personal data: information relating to an identified or identifiable individual, including special category and safeguarding information.
- Artificial intelligence (AI): systems that generate, transform, summarise, transcribe, classify or otherwise process content, including generative AI.
- Safe adult: a trusted adult whom a child can approach for help; in school this will normally be a member of staff.

4. Core acceptable-use expectations

All users must use technology lawfully, safely and respectfully. The following are unacceptable and may result in action under safeguarding, behaviour, staff conduct, disciplinary, data protection or other relevant procedures:

- accessing, creating, storing, sending or sharing illegal, pornographic, obscene, violent, hateful, extremist, terrorist, discriminatory or otherwise harmful material;
- bullying, harassment, intimidation, impersonation, humiliation, threats or unlawful discrimination;
- requesting, taking, creating, saving or sharing nude or semi-nude images or videos of anyone under 18, including AI-generated or manipulated content;
- attempting to gain unauthorised access to accounts, systems or data; creating, obtaining or using malware; damaging systems; or bypassing security, filtering or monitoring;
- sharing passwords, verification codes or access credentials;
- using school systems for gambling, scams, unauthorised commercial activity or unlawful financial gain;
- breaching copyright, intellectual property rights or academic integrity;
- sharing confidential, personal, safeguarding or school information without authority;
- connecting devices, installing software, apps, extensions or services without approval;
- using technology in a way that compromises safeguarding, professional boundaries, supervision, privacy, data protection or the learning environment.

5. Filtering and monitoring

Filtering and monitoring are safeguarding functions, not solely technical controls. Wouldham uses LGfL filtering and monitoring arrangements. These arrangements are designed to reduce access to illegal, inappropriate and harmful content without unreasonably restricting teaching, learning or access to appropriate support.

- The governing board will ensure the school meets current DfE filtering and monitoring standards and will review effectiveness at least annually.
- The DSL has lead responsibility for understanding filtering and monitoring processes and ensuring safeguarding concerns are acted upon.
- The IT providers support technical implementation, review and escalation.



- Staff will receive information and training on their responsibilities and must report filtering failures, inappropriate access, suspicious alerts or monitoring concerns promptly to a DSL and the IT provider.
- Filtering and monitoring will be considered across school devices, networks, cloud services, apps, mobile devices and approved AI tools.
- Monitoring of school-provided devices, accounts, systems and networks may continue when those services are used away from school. The school does not claim to monitor personal home internet, personal accounts or unrelated activity on personal devices.
- No filtering or monitoring system is foolproof. Education, supervision, reporting and safe relationships remain essential.

6. Mobile phones, smart technology and screen use

Wouldham is a smartphone-free primary school. Pupils must not use, access, display or check mobile phones or similar smart technology during the school day, including lessons, transitions, breaktimes, lunchtimes, clubs and school trips, unless a specific exception or reasonable adjustment has been agreed by the Headteacher/DSL.

- Pupils in Years 5 and 6 who walk to or from school independently may bring a basic non-internet-enabled mobile phone for safety. It must remain switched off and stored/handed in according to the school's agreed arrangements.
- Smartphones, smart watches, tablets, internet-enabled trackers and other personal smart devices are not permitted for pupils in school or on school trips unless a specific reasonable adjustment or exception has been formally agreed, risk assessed, recorded and communicated.
- Parents/carers should contact pupils through the school office during the school day rather than through a child's device.
- Staff must model safe and professional technology use. Personal phones and wearable devices must not compromise supervision, safeguarding, confidentiality, professional boundaries or the learning environment and must be used in line with the Common Sense Code.
- Personal devices must never be used to take images or recordings of pupils.
- In EYFS, screen use will be planned, purposeful, age appropriate and supervised. It will support learning, development, communication or care and will not replace face-to-face interaction, play, physical activity, rest, care routines or real-world exploration.

7. Artificial intelligence (AI)

AI can support teaching, learning, communication and administration, but it can also create safeguarding, privacy, data protection, intellectual property, misinformation, bias and academic-integrity risks. Only school-approved AI tools may be used for school purposes and only in approved ways.

7.1 Staff use of AI

- Staff must not enter personal, sensitive, confidential, safeguarding, assessment, special-category information or identifiable pupil images into an AI tool unless the tool and purpose have been formally approved and the processing has been confirmed as lawful and appropriate.
- Any proposed new or changed use of AI or cloud services involving personal data must follow the school's approval process and, where required, a Data Protection Impact Assessment (DPIA).
- AI-generated material must be checked by a competent adult for accuracy, bias, appropriateness, copyright and safeguarding implications before it is used or shared.



- AI must not replace professional judgement, safeguarding decision-making, assessment decisions or direct support from safe adults.
- AI tools that record, transcribe, summarise or generate notes from meetings, lessons, training or online discussions require prior approval. Participants must be informed about what is captured, why, how it will be used/stored and who can access it.
- Staff remain responsible for work produced with AI and must report any concerning output, data disclosure or misuse.

7.2 Pupil use of AI

- Pupils may use AI only when a teacher or other safe adult has explicitly permitted an approved tool for a defined learning purpose.
- Pupils must not enter personal information about themselves or others into AI tools.
- Pupils must not use AI to create fake or manipulated images, voices, videos or messages about other people, to impersonate, bully, harass, humiliate or mislead.
- Pupils will be taught that AI outputs may be inaccurate, biased, harmful or misleading and must be checked against reliable sources.
- AI must not be used to present generated work as the pupil's own where this would undermine learning or assessment.

8. Staff, governors, volunteers and contractors

8.1 Accounts, communication and professional boundaries

- Use school-provided or formally approved accounts, devices and systems for school business.
- Do not use personal email addresses, personal phone numbers, personal profiles, private messaging apps or gaming accounts to communicate with pupils or families unless a specific arrangement has been formally approved, risk assessed and recorded.
- Do not add, follow, accept or respond to friend requests or direct personal online communication from current pupils. Contact with former pupils or parents/carers must not blur professional boundaries.
- Discuss any pre-existing personal relationship that may affect professional boundaries with the DSL/Headteacher.
- School email must be used for work purposes. Multi-factor authentication must be enabled where available/required.
- Digital communication must be professional, factual and capable of appropriate scrutiny.

8.2 Personal devices and social media

- Personal device use on site must comply with the Common Sense Code and must not take place in a way that distracts from supervision or duties.
- Staff must not use personal devices to photograph, film or record pupils.
- Staff must use privacy settings carefully but must understand that privacy settings do not remove professional responsibilities.
- Staff must not post confidential information, discuss pupils or colleagues inappropriately, or publish content that compromises safeguarding, professional boundaries or the school's reputation.
- Concerns about online harassment, bullying or intimidation of staff should be preserved as evidence and reported through school procedures. Legitimate criticism, complaints and safeguarding reports remain able to be raised through appropriate routes.



8.3 Data and system security

- Lock/log out of devices when unattended and protect equipment from loss or theft.
- Use secure authentication. Do not share passwords, passkeys, verification codes or credentials. Passwords should not be changed routinely unless required or suspected to be compromised.
- Take care with links and attachments and report suspected phishing or malicious content to the IT provider.
- Do not install unauthorised software, browser extensions, hardware or services.
- Process personal data only through approved systems. Personal/sensitive school information must not be stored on personal devices.
- Report lost devices, lost data, suspected data breaches, malware or unauthorised access immediately to the Headteacher/DSL, IT provider and DPO as appropriate.

9. Pupils

9.1 Access and supervision

- School computers, laptops, tablets and online services are provided to support learning and are used with age-appropriate supervision.
- Pupils must use only the websites, tools, search engines, accounts and AI tools selected or approved by staff.
- Pupils must not attempt to bypass filters, change settings without permission or access another person's files or account.
- Pupils are taught to protect personal information and passwords, to behave kindly and respectfully online, to question whether online information is true, and to tell a safe adult if anything worries, frightens, confuses or upsets them.
- Age- and ability-appropriate AUP statements are provided in the appendices. Reasonable adjustments will be made so pupils with SEND or communication needs can understand and follow expectations.

9.2 Searching, confiscation and device examination

Searching, confiscation and any examination of a pupil device will be carried out only where lawful, necessary and proportionate and in line with current DfE guidance, the Behaviour Policy and safeguarding procedures. The DSL/deputy will be informed where a search reveals or is prompted by a safeguarding risk.

If staff suspect a device contains an indecent image of a child, they must not view, copy, print, share, store or save the image. The device should be secured and the incident reported immediately to the DSL/deputy, who will follow current DfE and UKCIS guidance. Potential evidence of an offence must not be deleted.

9.3 Online behaviour outside school

Where online behaviour outside school affects the safety or wellbeing of a pupil, member of staff or another person, disrupts the safe operation of the school, or raises a safeguarding, behaviour or potentially unlawful concern, the school may respond under its safeguarding and behaviour procedures. Any response will be fair, necessary and proportionate.

10. Parents and carers

- Parents/carers are encouraged to support safe, kind, lawful and responsible technology use and to discuss the pupil AUP with their child.
- Parents/carers should use the school office if they need to contact their child during the school day.



- The school will communicate what pupils are expected to do online and, where relevant, who from school they will interact with.
- Parents/carers will be given accessible information about filtering and monitoring. Monitoring is proportionate and does not extend to unrelated activity on personal devices, personal accounts or home internet.
- Parents/carers should raise safeguarding concerns, complaints or other issues through the school's established routes. The AUP does not prevent legitimate criticism, complaints, safeguarding reports or lawful communication.
- Parents/carers should not create or share content that targets, threatens, bullies, harasses or risks harm to a child, family, staff member or other member of the school community.

11. Data protection, privacy and information security

- Personal data will be processed fairly, lawfully and transparently, for specified purposes, kept no longer than necessary and protected by appropriate security.
- Access rights will be role-based and reviewed regularly. Users must report access they have received in error.
- School devices and systems will use appropriate encryption, firewalls, security updates, anti-malware and authentication controls.
- Portable or removable data must be protected using school-approved methods.
- School data must not be copied to unapproved personal devices, USB drives, cloud services or apps.
- Any data breach or suspected breach must be reported immediately in line with the Data Protection Policy and breach procedure.

12. Cyber security

- The school will provide annual cyber-security awareness training and induction for new staff.
- Critical data will be backed up in line with the school/IT provider's recovery arrangements and backups will be protected and tested.
- Access permissions and administrator rights will be reviewed regularly.
- The school will maintain and test an incident response plan and will work with its IT providers, DPO, local authority and relevant agencies as required.
- The school will not pay or engage with ransom demands as a routine response to ransomware.
- Supply-chain and third-party security will be considered when procuring services.

13. Internet and Wi-Fi access

The school's wireless internet is secured and filtered. Separate access arrangements are maintained for pupils/staff and guests where appropriate. Pupils access Wi-Fi only through approved school devices and under staff supervision.

- Parents/carers and visitors do not receive Wi-Fi access as a matter of course. Access may be authorised where needed for an official school purpose or multi-agency work.
- Wi-Fi credentials must not be shared with unauthorised users.
- Guest/personal devices connected to school Wi-Fi remain subject to filtering and may have network activity monitored for safeguarding, security and policy compliance. This does not give the school access to unrelated content held on the personal device.
- The school may restrict or withdraw Wi-Fi access to protect safeguarding, security, network reliability or fair use.



14. Images, recordings and remote/online learning

- Images and recordings of pupils may only be taken using school-provided or formally approved equipment and in accordance with the school's image-use, safeguarding and data-protection arrangements.
- Personal devices must not be used by staff, visitors or volunteers to take pupil images or recordings.
- Remote/online learning and communication must use school-approved systems and professional accounts.
- Platforms will be assessed for safeguarding, privacy, age restrictions, access controls, chat, screen sharing, recording, retention and reporting arrangements.
- Any recording of online sessions must have a clear, approved purpose and lawful basis, with participants informed appropriately.

15. Reporting concerns and responding to breaches

Safeguarding and online-safety concerns must be reported to a DSL immediately. Technical/security concerns should also be reported to the school's IT providers. Data protection incidents should be reported promptly to the Headteacher and DPO. Staff should report concerns even where they appear minor or accidental and should seek advice before acting if unsure.

- Pupil breaches may be managed under the Behaviour Policy and safeguarding procedures, with education and support as well as proportionate sanctions.
- Staff breaches may be considered under safeguarding, low-level concerns, allegations, staff conduct and disciplinary procedures.
- Where a concern may meet the harm threshold, the school will follow local allegations procedures and seek advice/referral to the LADO as appropriate.
- Where criminal activity may have occurred, the police or other relevant agency may be informed.
- Visitors/volunteers may have access withdrawn and concerns may be referred to their employer/organisation or relevant agency.

16. Monitoring, governance and review

The Headteacher/DSL, supported by the IT providers and DPO, will monitor implementation. The governing board will approve the policy and receive assurance about filtering and monitoring, safeguarding, cyber security and compliance. The policy will be reviewed at least annually and sooner following significant changes to legislation, statutory guidance, technology use, school systems, safeguarding practice or emerging risk.

17. Related school policies

- Child Protection and Safeguarding Policy 2026/27
- Common Sense Code / Staff Code of Conduct
- Behaviour / Nurture Behaviour Policy
- Data Protection and Information Security policies
- Online Safety arrangements
- Mobile Phone / Smart Technology expectations
- Parent Code of Conduct and Complaints Procedure
- Remote/Online Learning arrangements
- Image/photography and social media guidance
- SEND and reasonable adjustment procedures



DRAFT



Appendix 1: EYFS and Key Stage 1 pupil AUP

These simple statements should be discussed with children in an age-appropriate way. Visuals and reasonable adjustments should be used where helpful.

- I only go online when a grown-up at school says I can.
- I ask before I click on links or things online.
- I am kind and friendly online.
- I keep information about me and my passwords safe.
- I know school can check what I do on school computers and tablets to help keep me safe.
- If something online makes me worried, unhappy or confused, I stop and tell a grown-up.
- I follow the school rules about phones and smart devices.
- I have talked about these rules with my parent/carer.

Appendix 2: Key Stage 2 pupil AUP

I understand that these rules help keep me and other people safe and happy when using technology at school and when using school systems at home.

- I will be kind and respectful online and will not use technology to upset, frighten, embarrass, bully or impersonate anyone.
- I will only use websites, search tools, apps and accounts my teacher has chosen or allowed.
- I will keep personal information and passwords private and will not access or change another person's files or account.
- I will not try to bypass the school internet filter or change device settings unless a member of staff allows me.
- I know school-provided devices, accounts, systems and networks may be monitored to help keep people safe, including when I use them away from school.
- I know that not everything online is true. I will check information using other reliable sources or ask a safe adult.
- I will credit sources and will not copy someone else's work and pretend it is mine.
- I will only use AI tools when my teacher says I may. I will not put personal information into AI or use AI to make fake images, voices, videos or messages about people.
- If AI or anything else online shows me something worrying, rude, violent, confusing or unsafe, I will stop and tell a safe adult.
- I will only take or share pictures or recordings when I have permission and it is safe to do so.
- I will follow Wouldham's smartphone-free rules. If I am a Year 5/6 independent walker and bring an agreed basic non-internet phone, I will keep it switched off and follow the school storage/hand-in arrangements. I will not bring a smartphone, smart watch or other personal smart device unless a specific exception has been agreed.
- If someone online asks to meet me, or if something makes me uncomfortable or worried, I will tell a safe adult straight away.
- I understand that if I do not follow these rules, the school will respond in line with its Behaviour and Safeguarding policies.



Appendix 3: Parent/Carer AUP acknowledgement

Parents/carers are important partners in helping children use technology safely. By signing, I confirm that I have read the school's AUP and discussed the relevant pupil expectations with my child.

- I will support my child to use technology safely, kindly, lawfully and responsibly and will encourage them to seek help if something online worries them.
- I understand that school-provided devices, accounts and systems may be filtered and monitored proportionately, including when used away from school, but that the school does not monitor unrelated personal devices, accounts or home internet.
- I will support Wouldham's smartphone-free approach and will contact my child through the school office during the school day.
- I understand that any exception or reasonable adjustment for a personal device must be agreed with the school and recorded.
- I will support the school's rules concerning social media, images, recordings and AI.
- I will raise concerns, complaints or safeguarding matters through the school's established routes and will communicate respectfully online.
- I understand that online behaviour affecting safeguarding, wellbeing or the safe operation of the school may be considered under relevant school procedures.

Appendix 4: Staff, Governor, Volunteer and Contractor AUP

I understand that technology use connected to my role must be professional, lawful, ethical, safe and open to appropriate scrutiny. I agree to:

- use school-provided or approved systems, accounts and devices for school business and maintain professional boundaries in all digital communication;
- protect passwords, verification codes, data and devices and report phishing, malware, lost data, unauthorised access or suspected breaches promptly;
- not use personal devices to photograph, film or record pupils;
- not use personal accounts, private messaging apps, gaming accounts or personal phone numbers to contact pupils or families unless formally approved, risk assessed and recorded;
- follow the school's filtering and monitoring arrangements and report any failure or concerning access to the DSL and IT provider;
- use only approved AI tools, check outputs carefully, and never enter personal, confidential, safeguarding or special-category information unless the tool and processing have been formally approved;
- not allow technology, personal phones or wearables to compromise supervision, safeguarding, confidentiality, professional boundaries or the learning environment;
- report concerns involving online contact, devices, images, recordings, social media, AI, data protection or professional boundaries, even where they appear minor or accidental;
- follow the Child Protection Policy, Common Sense Code, Data Protection Policy and all related school procedures.



Appendix 5: Visitor and Volunteer technology expectations

Visitors and volunteers must use technology safely and in a way that protects pupils, staff, information and professional boundaries.

- Do not photograph, film or record pupils unless specifically authorised and using approved school equipment/arrangements.
- Keep personal phones and smart devices away during direct work with pupils unless specifically agreed for an essential purpose.
- Do not access or share confidential, personal or safeguarding information unless authorised for your role.
- Do not use personal accounts or contact details to communicate with pupils.
- Do not access illegal, harmful, offensive or inappropriate content or attempt to bypass school security, filtering or monitoring.
- Report any safeguarding, online-safety, filtering or technology concern immediately to a member of staff/DSL.
- Any Wi-Fi access is for the agreed purpose only and may be restricted, filtered and monitored proportionately.

Appendix 6: Guest Wi-Fi AUP

Where guest Wi-Fi is authorised, users agree to the following conditions:

- I will use the service lawfully and responsibly and only for the purpose for which access has been granted.
- I will keep my device secure and will not share Wi-Fi credentials or attempt to bypass filtering, monitoring or security controls.
- I will not use the Wi-Fi to access or share illegal/harmful content, compromise another person's safety or privacy, interfere with systems, or breach school policy.
- I understand that network activity may be monitored and recorded proportionately for safeguarding, security and policy compliance. This does not give the school access to unrelated information stored on my device.
- I will report inappropriate content, security concerns or filtering failures to the DSL or technical contact.
- I understand that access may be restricted or withdrawn where necessary.

Appendix 7: Quick staff checklist

- Use school accounts and approved systems.
- Lock devices; protect credentials; use MFA where available.
- No pupil photos/recordings on personal devices.
- No personal messaging/social/gaming contact with pupils.
- Report filtering failures and safeguarding concerns immediately.
- Use only approved AI; never paste sensitive/personal/safeguarding information into unapproved AI.
- Check AI output for accuracy, bias, copyright and safeguarding.
- Keep phones/wearables from compromising supervision or professional boundaries.
- Report phishing, malware, lost devices/data and data breaches promptly.
- If unsure, ask the DSL/Headteacher before using a new technology or communication route.