

Computing, E-Safety and Acceptable User Policy



RATIFICATION: Autumn 2026

DATE OF NEXT REVIEW: Autumn 2027

REVIEWED BY: Head of School

APPROVED BY: Local Governing Body

Stokesay Primary School

E-Safety & Acceptable Use Policy

Statutory Context

- Meeting Digital and Technology Standards in Schools and Colleges (DfE)
- Filtering and Monitoring Standards for Schools and Colleges (DfE)
- Cyber Security Standards for Schools and Colleges (DfE)

This policy should be read in conjunction with:

- Keeping Children Safe in Education (DfE, 2025)
- Working Together to Safeguard Children (latest version)
- Prevent Duty Guidance (Counter-Terrorism and Security Act, 2015, updated 2021)
- UK GDPR and Data Protection Act (2018)
- Teaching Online Safety in Schools (DfE, 2019)
- Shropshire Safeguarding Community Partnership (SSCP) guidance

This policy also links directly to the school's Safeguarding and Child Protection Policy, Behaviour Policy and Anti-Bullying Policy.

Responsibilities

- The member of SLT responsible for e-safety: Mr William Vaughan (Head of School / DSL)
- The Governor responsible for safeguarding and e-safety: Mrs Rose Patey
- The E-Safety Co-ordinator: Mr William Vaughan

The E-Safety Co-ordinator is responsible for developing the online safety curriculum (through Computing, RSHE and PSHE), staff training, recording and monitoring incidents, and liaising with the Local Authority and external agencies. They may also deliver workshops for parents.

All staff are responsible for safeguarding the school's ICT systems and modelling safe and responsible use of technology.

Acceptable Use Policies (AUPs)

- All members of the school community (pupils, staff, parents, governors, visitors) are expected to sign and follow an Acceptable Use Policy (appropriate to their role).
- AUPs are reviewed annually and stored centrally in case of breaches.
- Online safety teaching forms part of the Computing curriculum and is reinforced through RSHE and PSHE.

Legislation and Compliance

All users must comply with relevant law, including:

- Data Protection Act 2018 and UK GDPR
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

Breaches may be treated as misconduct or, in serious cases, criminal offences.

Internet, Email and Cloud Use

- All internet and email use must support teaching and learning.
- Personal use of email should be minimal and clearly marked as “personal.”
- School email accounts must be used for school business; personal accounts must not.
- Internet and email use is filtered, logged and monitored for safeguarding and data protection.

Artificial Intelligence (AI)

- The school recognises that Artificial Intelligence (AI) tools are increasingly accessible to pupils and staff.
- AI may be used to support teaching, learning and administrative functions where approved by school leaders.
- Staff remain responsible for the accuracy, appropriateness and safeguarding implications of any content generated by AI tools.
- Personal, sensitive or confidential information must not be entered into public AI platforms.
- Pupils will be taught age-appropriate awareness of AI, including the benefits, limitations and risks of AI-generated content.
- Staff should challenge misinformation, deepfakes and manipulated media as part of online safety education.

Photographs and Video

- Photos and video are classed as personal data under GDPR.
- Where images are used for education, public task is the lawful basis. For marketing, consent is required.
- Parents’ consent is collected on admission forms and recorded in SIMS.
- Only school-owned devices should be used to capture images. Images must be stored securely and deleted from devices as soon as possible.
- Parents are not permitted to record school events unless specifically authorised.

Mobile Phones and Personal Devices

- Staff mobile phones must be silent and out of sight during the school day unless in staff areas.
- Visitors must hand phones to the office unless required for a professional task.
- Pupils may only bring phones if authorised (e.g. Year 6 walking home independently) under the Mobile Phone Policy.

Security and Passwords

- Passwords must be strong, unique and changed termly.
- Staff must not share passwords.
- School systems are monitored and filtered.
- Staff using personal devices must ensure they are secure and not linked to school systems without authorisation.

Data Storage

- Staff must use encrypted devices or the school’s OneDrive/SharePoint system.
- USB devices should be encrypted.
- Personal data must not be stored on unencrypted devices.

Cyber Security

- Promote strong password security and multi-factor authentication where available.
- Ensure devices and software are regularly updated.
- Provide staff with awareness training regarding phishing, scams and cyber threats.
- Maintain secure backups of critical data.
- Report significant cyber incidents in accordance with relevant guidance and procedures.

Filtering and Monitoring

- The school maintains appropriate filtering and monitoring systems to help safeguard pupils online.
- Filtering systems are designed to block access to harmful and inappropriate content.
- Monitoring systems identify safeguarding concerns and potential misuse of technology.
- The DSL and Head of School receive appropriate information regarding serious incidents and concerns.
- Arrangements are reviewed regularly and governors receive assurance regarding effectiveness.

Reporting and Incidents

- All breaches of this policy must be recorded in SIMS and reviewed by the E-Safety Co-ordinator.
- Child protection concerns must be referred to the DSL immediately.
- Allegations against staff follow statutory safeguarding procedures and may involve the LADO.
- Evidence of incidents must be preserved. Online safety incidents, cyber security concerns and filtering or monitoring alerts will be reviewed by the DSL and recorded in accordance with safeguarding procedures where appropriate. Serious incidents may be referred to external agencies including the Local Authority, Police, CEOP or the Information Commissioner's Office where required.

Education and Training

****For Pupils:****

- Online safety is taught through Computing, RSHE and PSHE, and reinforced through assemblies.
- Pupils learn to recognise online risks, validate information, respect copyright, and challenge misinformation.
- Pupils are taught how to report concerns (trusted adult, CEOP button, Childline).

****For Staff:****

- Online safety is part of annual safeguarding and Prevent training.
- New staff receive induction training on the E-Safety Policy and AUPs.
- Additional CPD (e.g. CEOP training) is encouraged. Pupils are taught about online scams, fake news, misinformation, disinformation, deepfakes and the responsible use of AI technologies. Pupils are taught how algorithms, influencers and online platforms can affect decision making and wellbeing. Staff receive annual updates regarding emerging online risks, AI technologies, cyber security and filtering and monitoring expectations.

Social Media

- Pupils and staff must not use social networking during school hours (except in staff areas).
- Staff must never discuss school business or pupils on personal social media.
- Professional networking (e.g. subject forums) is permitted.
- Staff must not accept friend requests from pupils or parents. Staff must not share school photographs, pupil information or school business using personal messaging applications or social media platforms. Any school social media accounts must be managed through authorised school systems and overseen by school leaders.

Monitoring and Review

- The DSL/Head of School monitors online safety incidents and reports to governors.
- Governors review this policy annually.
- The policy is updated in line with new statutory guidance.

Appendix 1: Acceptable User Policies

Parent/Carers Agreement

- I have read and discussed the Acceptable Use Policy with my child.
- I know that my child will receive digital (online) safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that the use of the internet using school equipment is monitored for safety and security reasons and to safeguard both my child and the schools systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task, particularly with new technologies and sudden online trends.
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted. This includes concerns that inappropriate online material viewed at home is being discussed in school. I also understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the school's behaviour and anti-bullying policy.
- I, together with my child, will support the school's approach to digital safety and will not deliberately upload or publish any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community, either on school or home devices. I will not name or identify members of staff on social media and any discussion of school will be professional and in line with the ethos of this policy.
- I will ensure that my child does not bring any device to school (including smartphones, smartwatches or cameras) that have the ability to photograph, video or audio record, unless by prior written agreement from Mr. O'Malley and Mr. Vaughan. Any such agreement would be fully risk assessed.
- I know that I can speak to the school safeguarding team, my child's teacher or the Head Teacher if I have any concerns about digital safety.
- I will visit the school website and the Computing curriculum page [Computing](#) for more information about the school's approach to digital safety.
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/online-safety, www.internetmatters.org, www.saferinternet.org.uk, and www.childnet.com for more information about keeping my child(ren) safe online.

- I will support the school and my child by sharing responsibility and role modelling safe and positive online behaviour for my child and by discussing online safety with them when they access technology at home.
- When communicating with school electronically, either via email or through learning portals such as Tapestry, all communication will be polite, professional and with a view to building a supportive collaboration for the benefit of pupils.

Key Stage 1 Pupil Agreement

- I will look after all the school IT equipment and use it properly.
- I will only share my username or password with trusted adults.
- I will tell an adult if I see anything which upsets me.
- I will always ask before downloading from the internet or using files I have brought into school because I understand the risks from virus infections.
- Any work I upload to the internet will be my own.
- I will only take a photograph or video of someone if they say it is alright.
- All of the messages I send will be polite.
- I will not post anything online which upsets other people.
- I will use a safe online name and not give away my personal information or talk to people I do not know using the internet.
- I understand that the school may check my use of IT and talk to my parent or carer if they are worried about my online safety.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school.

Pupil name.....

I confirm that I have read this policy with my child and have understood this policy.

Signed.....

Relationship to child.....

Key Stage 2 Pupil Agreement

- I will take care when using the school IT equipment and use it responsibly.
- I will keep my passwords private unless I need to share them with a trusted adult.
- I will inform an adult if I see or receive any unpleasant text, images or messages.
- I will not interfere with anyone else's passwords, settings or files on the computer.
- I will be careful when downloading material from the internet or using material I have brought into school because I understand the risks from virus infections.
- Any work I upload to the internet will be my own.
- I know that if I want to take a photograph or video of somebody, I will need their permission and my teacher's permission.
- I will not bring any device into school that can take photos, videos or audio recordings unless Mr. O'Malley and Mr. Vaughan have given written agreement.
- Any messages I post online or send in an email will be polite and responsible. I will always ask myself "how would I feel if my parents or the other person's parents saw it?"
- I will not send or forward messages or create material which is deliberately intended to upset, embarrass or scare other people.
- I know I must take care about giving away my personal information and making contact with people I do not know when using the internet.

- I understand that the school may check my use of IT and contact my parent/carer if they are concerned about my online safety.
- I recognise that if online activities at home make me angry, cross or upset when I get into school and affect my work or playtimes, my teacher might need to speak to my parents/carers.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may happen even if the activity was done outside school.

Pupil name.....

I confirm that I have read this policy with my child and have understood this policy.

Signed.....

Relationship to child.....

Staff Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
 - I will not use personal email addresses on the school's ICT systems without first discussing it with a member of SLT.
 - I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
 - I will ensure that my data is regularly backed up, in accordance with relevant school policies.
 - I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
-
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
 - I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
 - I will not disable or cause any damage to school equipment, or the equipment belonging to others.
 - I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.

- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

Name.....

I confirm that I have read and understand this policy.

Signed.....

Appendix 2: General consent form

Basic Information

Allergies and dietary information:

Permissions please tick.

Photograph and first name on school website, digital platforms e.g. tapestry, newsletter and displays around school:

☐

Photograph and video imaging with first names on Trust newsletters, sports events and local press :

☐

Copyright permission of work produced e.g. for displays, competitions :

☐

Sex Education in Key Stage 2

☐

Accessing the internet in line with our acceptable use policy:

☐

If any of your child's circumstances change (e.g. relating to medical conditions/allergies), you must inform the school.

Please sign and date

Signed:..... Date:.....

Basic Information

Name :

Contact details in emergency :

1st contact

2nd Contact

Phone number to be used for

'Text to parents ' purpose:

Email address to be used for parents letters :

Any Medical conditions :

If Asthmatic permission to use an emergency inhaler:

Doctors and Medical centre details: