Truro and Penwith Academy Trust

Pensans CP School

Acceptable Use Policy (AUP) for Information Technology

Updated to reflect guidance and standards in force from September 2026

Review Summary

Approved By:	Headteacher
Approval Date:	September 2026
Next Review Date:	September 2027

Contents

This policy refers to, and should be read alongside, the following legislation, statutory guidance and standards. The titles are clickable links to the official source.

- Data Protection Act 2018.
- UK General Data Protection Regulation (UK GDPR).
- Data (Use and Access) Act 2025 and associated data protection changes in force from July 2026.
- Computer Misuse Act 1990.
- Human Rights Act 1998.
- Freedom of Information Act 2000.
- Education and Inspections Act 2006.
- Education Act 2011.
- Keeping Children Safe in Education 2026 (statutory guidance).
- Searching, screening and confiscation in schools (DfE).
- Behaviour in schools (DfE).
- Mobile phones in schools (DfE) – statutory guidance in force from September 2026.
- DfE Meeting digital and technology standards in schools and colleges, including the core standards for filtering and monitoring, cyber security and digital leadership and governance.
- DfE Filtering and monitoring: core standard.
- DfE Cyber security: core standard.
- DfE Generative artificial intelligence (AI) in education.
- DfE Generative AI: product safety standards.
- DfE Data protection in schools, including guidance on generative AI and data protection.
- National Cyber Security Centre (NCSC) guidance and cyber security standards for schools and colleges.
- DfE Cyber Security Hub: resources and support.
- UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes.
- Equality Act 2010, including duties relating to discrimination and harassment.
- DfE Preventing bullying.
- DfE Preventing and tackling bullying and harassment of school staff.
- DfE School and college security guidance.

1. Introduction and aims

Information and communications technology (ICT), digital technology and online services are integral to the way Pensans CP School works. They support teaching and learning, communication, administration, safeguarding and the preparation of pupils for life in a digital society.

Technology also creates risks to safeguarding, privacy, cyber security, wellbeing and the reputation of the school. This policy sets out the acceptable use of the school's technology, systems, devices, networks and online services and the behaviour expected of everyone who uses them.

This policy aims to:

- Set clear rules for the safe and responsible use of school ICT and digital resources by staff, pupils, governors, volunteers, contractors, visitors and parents/carers where relevant.
- Promote respectful, safe and responsible behaviour online and offline.
- Support the school's safeguarding, online safety, behaviour, data protection and cyber security arrangements.
- Protect pupils, staff, families and the school from harmful, illegal, inappropriate or discriminatory content and conduct.
- Support pupils to develop the knowledge and skills needed to use technology safely, critically and effectively.
- Provide clear expectations for the use of generative artificial intelligence (AI) and other emerging technologies.
- Reduce the risk of cyber attacks, data breaches, unauthorised access, fraud and disruption to school operations.
- Make clear that use of school systems may be filtered and monitored for safeguarding, security, operational and legal purposes.

This policy covers all users of the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. It applies to school-owned devices and systems and, where relevant, to personal devices when they are used to access school systems, connect to the school network or engage in behaviour that affects the school community.

Breaches may be dealt with under the school's Behaviour Policy, Staff Code of Conduct, safeguarding procedures, disciplinary procedures, complaints procedures or other relevant policies.

2. Relevant legislation and guidance

This policy refers to, and should be read alongside, the following legislation, statutory guidance and standards:

- Data Protection Act 2018.
- UK General Data Protection Regulation (UK GDPR).
- Data (Use and Access) Act 2025 and associated data protection changes in force from July 2026.
- Computer Misuse Act 1990.
- Human Rights Act 1998.
- Freedom of Information Act 2000.
- Education and Inspections Act 2006.
- Education Act 2011.
- Keeping Children Safe in Education 2026 (statutory guidance).
- Searching, screening and confiscation in schools (DfE).
- Behaviour in schools (DfE).
- Mobile phones in schools (DfE) – statutory guidance in force from September 2026.
- DfE Meeting digital and technology standards in schools and colleges, including the core standards for filtering and monitoring, cyber security and digital leadership and governance.
- DfE Generative artificial intelligence (AI) in education.

- DfE Generative AI: product safety standards.
- DfE Data protection in schools, including guidance on generative AI and data protection.
- National Cyber Security Centre (NCSC) guidance and cyber security standards for schools and colleges.
- UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes.
- Equality Act 2010, including duties relating to discrimination and harassment.

3. Definitions

Term	Definition
ICT facilities	All facilities, systems and services including network infrastructure, computers, laptops, tablets, phones, interactive technology, software, websites, cloud platforms, apps, online services and any future technology provided or authorised by the school.
Users	Anyone authorised to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
Personal device	A device owned by an individual rather than the school, including a mobile phone, tablet, laptop, smartwatch or USB storage device.
Personal use	Use or activity not directly related to a user's employment, study, school role or another purpose authorised by the school.
Authorised personnel	Staff or technical support personnel authorised by the school or Trust to administer, maintain, filter, monitor or support ICT facilities.
Materials	Files and data created, stored, accessed or transmitted using school ICT, including documents, photographs, audio, video, emails, messages, web pages and social media content.
Generative AI	Technology that creates new content such as text, images, audio, video, code or other digital material in response to prompts or other inputs.
Filtering	Technical controls designed to prevent users accessing illegal, inappropriate or potentially harmful online content.
Monitoring	Processes used to identify, record, review and respond to activity or content on school systems for safeguarding, security, operational and legal purposes.
Cyber incident	An event affecting the confidentiality, integrity or availability of systems, networks or data, including malware, phishing, ransomware, unauthorised access or data loss.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. This list is not exhaustive. The Headteacher, in consultation with the Trust and relevant professionals where appropriate, may determine that other behaviour constitutes unacceptable use.

- Using school ICT to breach copyright, intellectual property rights or licensing requirements.
- Using technology to bully, harass, threaten, intimidate, stalk or discriminate against another person.
- Using technology to create, access, store, send or share pornographic, abusive, extremist, hateful, discriminatory, violent or otherwise harmful material.
- Sharing or requesting nude or semi-nude images or videos involving children or young people. Any such concern must be referred immediately to the DSL; staff must not copy, save, forward or otherwise distribute such material.
- Accessing, creating or distributing content that is racist, antisemitic, Islamophobic, homophobic, transphobic, misogynistic or discriminatory on any other unlawful or harmful basis.
- Engaging in illegal conduct, fraud, phishing, scams, gambling or activities intended to facilitate crime.
- Attempting to bypass, disable or interfere with filtering, monitoring, security or safeguarding systems.
- Attempting to gain unauthorised access to networks, accounts, files, devices, data or administrative functions.
- Sharing passwords, authentication codes, security credentials or access tokens with another person.
- Connecting unauthorised devices, software, applications, storage media or online services to school systems.
- Installing software, browser extensions, apps, scripts or other tools without appropriate authorisation.
- Causing intentional damage, disruption, deletion or alteration to school ICT equipment, systems or data.
- Sharing confidential or personal information without authorisation.
- Using technology in a way that could bring the school, Trust or members of the school community into serious disrepute.
- Using school ICT for private business or commercial activity without authorisation.
- Using another person's account or impersonating another person.
- Uploading school data or confidential information to unapproved websites, cloud services or AI tools.
- Using AI to fabricate evidence, create deceptive communications, impersonate people, or produce harmful or discriminatory content.
- Using generative AI to complete pupils' assessed work or homework where the work is then presented as entirely the pupil's own work.
- Using technology in a manner inconsistent with safeguarding, behaviour, staff conduct, data protection or other school policies.

4.1 Exceptions from unacceptable use

Where school ICT is required for a legitimate educational, safeguarding, technical, administrative or professional purpose that might otherwise appear to fall within this section, an authorised member of staff may approve its use. Any such use must be proportionate, risk assessed where appropriate and consistent with relevant law and school policy.

Generative AI may be used by pupils only where the school has specifically authorised the tool and activity, and where:

- the tool is suitable for the pupil's age and any applicable age restrictions are followed;
- the activity has a clear educational purpose and is supervised appropriately;
- the tool has appropriate safety, filtering, monitoring and privacy arrangements;
- pupils do not enter personal, confidential or sensitive information;
- pupils are taught to check accuracy, bias, reliability and source information;
- AI-generated work is identified or acknowledged where required by the teacher or task instructions;
- the use of AI does not replace the pupil's own thinking, creativity or learning.

4.2 Sanctions

Pupils and staff who breach this policy may face action in line with the Behaviour Policy, Staff Code of Conduct, disciplinary procedures or safeguarding procedures. Access to systems may be restricted where necessary to protect users, data or school operations. Serious incidents may be referred to the Trust, police, safeguarding partners, the Information Commissioner's Office or other relevant agencies.

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

5.1 Access to school ICT facilities and materials

The school, supported by TPAT IT Support, manages access to ICT systems, devices, applications, files and services. Staff will normally be provided with individual accounts and must use their own credentials. Access should be based on role and need and reviewed when staff change role or leave.

- Never use another person's account or allow another person to use yours.
- Report suspected compromised accounts, lost devices, accidental access or incorrect permissions immediately.
- Lock screens when devices are unattended and log out when appropriate.
- Use multi-factor authentication where provided and required.
- Use the Trust-approved password manager or other approved secure method for storing credentials.
- Do not write passwords where pupils or unauthorised people can access them.

5.1.1 Use of phones and email

- School email accounts and approved communication platforms must be used for work-related communication.
- Personal email addresses, personal messaging accounts and personal social-media accounts must not be used for routine communication with pupils.
- Staff must not give pupils or parents/carers their personal phone number unless there is a specific, authorised reason and appropriate safeguarding controls.
- Work-related communications should be professional, factual and proportionate and may be retained or disclosed where legally required.
- Sensitive or confidential information must only be shared using approved secure systems and in accordance with the Data Protection Policy.
- If information is sent to the wrong person, or a device/account is lost or compromised, staff must report the incident immediately and follow the school's data breach procedure.

5.2 Personal use

Limited personal use of school ICT may be permitted where authorised, reasonable and not disruptive. It must not take place in a way that compromises safeguarding, confidentiality, productivity or the security of school systems.

- Personal use must not occur during teaching or other duties where attention is required.
- Personal use must not involve inappropriate, illegal or harmful content.
- Personal files should not be stored on school systems unless specifically authorised.
- Staff should assume that use of school systems may be logged or monitored.
- Personal devices used in school must comply with the school's mobile phone and device arrangements.

5.2.1 Personal social media accounts

- Staff must maintain professional boundaries online.
- Staff must not accept or initiate inappropriate online relationships with pupils.

- Staff should review privacy and security settings regularly and consider the permanence and public nature of online content.
- Staff should not post confidential information, photographs or comments about pupils or colleagues without authorisation.
- Where personal online activity creates a safeguarding, professional conduct or reputational concern, the school may take action in accordance with relevant procedures.

5.3 Remote access

Remote access is permitted only through approved systems. Staff must protect school information from being viewed, lost or accessed by others and should avoid working with confidential information in public or insecure environments.

5.4 School social media accounts

Only authorised staff may manage or post to official school or Trust social-media accounts. Content must follow the school's communications, safeguarding, image-use and data-protection requirements. Passwords and recovery details must be securely managed and not shared informally.

5.5 Monitoring and filtering

The school filters and monitors ICT use to help safeguard children, protect users and systems, investigate suspected misuse, maintain effective operations, meet legal obligations and respond to security incidents. Monitoring will be proportionate, lawful and aligned with the school's risk assessment and privacy obligations.

Pensans uses Netsweeper and On Guard as part of its filtering and monitoring arrangements. The named school contacts for these systems are maintained by the school and Trust and will be updated when responsibilities change.

6. Pupils

6.1 Access to ICT facilities

Pupils may use school ICT and online services when authorised and, where appropriate, under staff supervision. Pupils must follow teacher instructions, the age-appropriate AUP and the school's online safety expectations.

- Use only accounts and devices you are authorised to use.
- Keep passwords and login details private.
- Tell an adult if you see something upsetting, frightening, inappropriate or suspicious.
- Do not deliberately search for, create, save or share harmful material.
- Do not bypass filters or monitoring.
- Do not take or share photographs, recordings or personal information about others without appropriate permission.
- Treat people respectfully online and offline.

6.2 Search and deletion

The Headteacher and authorised staff may exercise statutory powers to search pupils and their possessions where there are reasonable grounds to suspect that a pupil has a prohibited or harmful item, in accordance with current DfE Searching, screening and confiscation guidance and the Behaviour Policy.

Where a device is confiscated, staff will act proportionately and only examine content where there is a lawful and appropriate reason. Staff will preserve potential evidence where an offence may have occurred and will involve the DSL where a safeguarding concern arises.

If a device may contain a nude or semi-nude image of a child, staff must not view, copy, save, print or share the image. The device and concern must be referred immediately to the DSL, who will follow the latest safeguarding guidance.

6.3 Unacceptable use of ICT and the internet outside of school

The school may take action where pupils use technology outside school in a way that affects the safety, wellbeing, education or reputation of members of the school community or the orderly running of the school.

- Cyberbullying, harassment, threats or discriminatory abuse.
- Sharing confidential school information or another person's personal information.
- Creating or sharing harmful, illegal, sexualised or extremist content.
- Attempting to gain unauthorised access to school systems.
- Using technology to threaten or encourage violence or criminal activity.

6.4 Mobile phones and smart technology

In line with the DfE statutory guidance on mobile phones in schools, Pensans operates a school-day expectation that pupils do not use mobile phones or other communication/smart technology during the school day, including lessons, breaks and lunchtime, except where a specific exception, reasonable adjustment or authorised educational use applies.

- Pupils must follow the school's arrangements for storing or securing phones when they arrive at school.
- Phones and smart devices must not be used to photograph, film, record, message or contact others during the school day unless specifically authorised.
- Where a pupil has a medical, SEND or other legitimate need requiring access to a device, the school will make appropriate arrangements.
- Breaches will be dealt with in line with the Behaviour Policy and mobile phone arrangements.

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's internal ICT facilities as a matter of course. Where a parent/carer is authorised to use school facilities in an official capacity, they must comply with the relevant parts of this policy.

7.2 Communicating with or about the school online

- Communicate respectfully with school staff, pupils, governors and other families.
- Do not use social media to threaten, harass, intimidate or target members of the school community.
- Do not publish confidential information or images of children without appropriate permission.
- Concerns and complaints should normally be raised through the school's published procedures rather than through public social media.

7.3 Communicating with parents/carers about pupil activity

Where pupils are asked to use online services for learning, the school will provide appropriate information to parents/carers. Parents/carers should encourage children to tell a trusted adult if they are contacted unexpectedly, asked to use an unapproved app or service, or encounter anything that makes them feel unsafe.

8. Data security

The school and Trust are responsible for maintaining appropriate technical and organisational measures to protect personal data, school systems and users. Everyone who handles personal data has a responsibility to keep it secure.

- Use only approved systems for storing and processing school information.
- Do not upload personal, confidential or sensitive school information to unapproved websites, apps, cloud services or AI tools.
- Check recipients carefully before sending messages or attachments.
- Use secure methods for transferring sensitive information.
- Lock devices when unattended.
- Report loss, theft, accidental disclosure, phishing or suspected data breaches immediately.
- Follow the school's retention, disposal and data protection arrangements.

8.1 Passwords

- Use strong, unique passwords or passphrases.
- Never share passwords or authentication codes.
- Use multi-factor authentication where available.
- Use the approved password manager where one is provided.
- Report compromised credentials immediately and change them when instructed.

8.2 Software updates, firewalls and anti-malware

School-managed devices and systems should receive security updates and protective controls in line with Trust IT arrangements. Users must not disable security software or circumvent administrative controls.

8.3 Data protection

Personal data must be processed lawfully, fairly and securely and only for appropriate purposes. Users must follow the school/Trust Data Protection Policy and the instructions of the Data Protection Officer or data protection lead.

The school will also consider the data protection implications of new technology, including AI tools, monitoring systems, apps and cloud services. Where required, appropriate due diligence, contracts, risk assessments and Data Protection Impact Assessments will be completed before use.

8.4 Access to facilities and materials

Access rights will be based on role and need. Users must not attempt to access systems, files or data to which they have not been authorised. Permissions should be reviewed when staff change roles and when accounts are no longer required.

8.5 Encryption and removable media

Where appropriate, school devices and systems will use encryption. Removable media and personal devices must not be used to store or transfer school data unless specifically authorised and appropriately secured.

8.6 Generative AI and personal data

Staff and pupils must not enter personal data, special category data, safeguarding information, confidential school information or identifiable pupil information into public or unapproved generative AI tools. AI outputs must be checked for accuracy, bias, safety, confidentiality and appropriateness before being used.

9. Protection from cyber attacks

The school will work with TPAT and its IT providers to maintain proportionate cyber security controls. The DfE's digital and technology standards identify cyber security as a core standard and the NCSC provides further practical guidance.

The school will seek to:

- Maintain an annual cyber risk assessment and review cyber risks regularly.
- Maintain a cyber awareness plan and provide suitable training for staff.
- Use layered security controls including firewalls, anti-malware, filtering, monitoring and secure authentication.
- Use multi-factor authentication for appropriate services.
- Restrict administrative privileges and regularly review user access.
- Keep supported software, operating systems and security controls up to date.
- Maintain secure and tested backups of critical data and consider resilience against ransomware.
- Maintain a cyber incident response process, including escalation and communication arrangements.
- Test or exercise incident response arrangements periodically and after significant changes or incidents.
- Consider cyber security when procuring suppliers, software and online services.
- Work towards the DfE digital and technology core standards and relevant NCSC/Cyber Essentials expectations.

9.1 Recognising and reporting cyber incidents

Users must report immediately if they suspect:

- a phishing or suspicious email;
- a compromised password or account;
- malware or ransomware;
- unexpected loss of access to systems or files;
- a lost or stolen device containing school information;
- unauthorised access or unusual account activity;
- accidental disclosure of personal or confidential information;
- a suspicious payment request or change to bank details.

Users should not investigate beyond what is necessary to report the concern, should not pay a ransom or attempt to conceal an incident, and should follow the Trust's incident-response instructions.

10. Internet access, filtering and monitoring

Pensans recognises that children must be protected from harmful online content while also being given meaningful opportunities to learn how to use the internet safely and critically. Filtering and monitoring are therefore part of a wider safeguarding approach and do not replace adult supervision, education, clear expectations or pastoral support.

The governing body and school leadership are responsible for ensuring that appropriate filtering and monitoring arrangements are in place. The DSL has lead responsibility for understanding how filtering and monitoring operate and for ensuring that safeguarding concerns are escalated appropriately, with support from Trust IT and relevant leaders.

The school will:

- Identify and assign roles and responsibilities for filtering and monitoring.
- Review filtering and monitoring provision at least annually and after significant changes or incidents.
- Use filtering that blocks harmful and inappropriate content without unreasonably restricting teaching and learning.
- Maintain effective monitoring strategies proportionate to the school's safeguarding risks.
- Ensure staff with relevant responsibilities understand the systems and know how to escalate concerns.
- Provide routes for pupils and staff to report inappropriate or blocked content.
- Review alerts and logs and respond to safeguarding or security concerns promptly.
- Consider risks associated with emerging technologies, including generative AI and non-browser services.
- Ensure filtering and monitoring arrangements are considered when new systems, devices or online services are introduced.

10.1 Current school arrangements

The school's filtering and monitoring arrangements include Netsweeper and On Guard, supported through TPAT and the school's designated responsible staff. Technical details, contacts and configurations may change and are maintained through the school's operational ICT documentation and Trust arrangements.

The school uses a combination of physical supervision, internet/web monitoring and proactive technical monitoring. Alerts requiring rapid safeguarding action are escalated in accordance with the Child Protection and Safeguarding Policy.

10.2 Pupils

Pupil access to wireless and online services is controlled according to age, need, device and supervision. Pupils must not attempt to circumvent filtering or monitoring and must report content that appears inappropriate or has been incorrectly blocked.

10.3 Parents/carers and visitors

Parents/carers and visitors are not normally provided with access to the school's Wi-Fi. Where access is authorised for an official purpose, users must comply with the school's security and acceptable-use requirements. Staff must not share Wi-Fi credentials without authorisation.

11. Monitoring and review

The Headteacher, supported by the Trust IT team and relevant safeguarding leaders, will monitor implementation of this policy. The school will review whether its arrangements remain appropriate in light of technology, incidents, pupil needs, safeguarding risks, DfE guidance and Trust requirements.

- Filtering and monitoring will be reviewed at least annually and after significant incidents or changes.
- Cyber security risks and controls will be reviewed regularly.
- Staff will receive appropriate training and induction.

- The effectiveness of this policy will be considered alongside online safety, safeguarding, behaviour and data protection arrangements.
- The policy will be formally reviewed at least annually, and sooner if statutory guidance or technology changes materially.

The governing board is responsible for ensuring that appropriate oversight is in place.

12. Related policies

- Online Safety Policy
- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy
- Mobile Phone Policy / arrangements
- Equality Policy
- SEND Policy
- Complaints Policy
- Whistleblowing Policy
- Home Learning / Remote Education arrangements where applicable

Appendix 1: Social media guidance for staff

Social media is a personal activity, but staff remain responsible for maintaining professional boundaries and protecting pupils, colleagues and the reputation of the school. Content posted online can be copied, shared and retained even after deletion.

- Keep personal accounts appropriately private and review security settings regularly.
- Do not accept inappropriate friend/follow requests from current pupils.
- Do not communicate privately with pupils through personal social-media accounts or messaging services.
- Do not publish confidential information about pupils, families, staff or school business.
- Do not post photographs or recordings of pupils unless authorised through the school's image-use arrangements.
- Do not post comments that could reasonably be considered threatening, discriminatory, harassing or professionally inappropriate.
- Remember that a personal account can still affect professional relationships and trust.
- If you are unsure whether something is appropriate, do not post it and seek advice from a senior leader.

What to do if a pupil contacts you on social media

- Do not engage in private conversation.
- Do not accept the request or move the conversation to another platform.
- Take appropriate evidence if there is a safeguarding or professional concern.
- Inform the Headteacher/DSL in accordance with school procedures.

What to do if you are harassed online

- Do not retaliate.
- Save appropriate evidence such as screenshots and dates.
- Report harmful content to the platform where appropriate.
- Tell a senior leader and seek advice on whether the matter is a safeguarding, disciplinary, legal or police concern.

Appendix 2: Acceptable Use Policy (AUP) for PARENTS

We ask adults involved in the life of Pensans School to support children in using technology safely, respectfully and responsibly. The same expectations about respect apply online as they do face to face.

I understand and agree that:

1. The school uses technology to support learning, communication, administration and safeguarding.
2. The school uses reasonable technical and educational measures to reduce children's exposure to harmful online content.
3. School systems, devices and networks may be filtered and monitored.
4. I will support my child to follow the school's AUP and online safety expectations.
5. I will encourage my child to tell a trusted adult if something online makes them worried, frightened or uncomfortable.
6. I will not encourage my child to use apps, games or services below their stated age restrictions.
7. I will model respectful behaviour online and will not use social media to threaten, harass or target school staff, pupils or families.
8. I will not share photographs, videos or personal information about other children without appropriate permission.
9. I will contact the school through appropriate channels rather than using public social media to resolve complaints.
10. I will support the school's arrangements for mobile phones and personal devices.
11. I will help my child understand that online content can be inaccurate, manipulated or generated by AI.
12. I understand that children should not enter personal or confidential information into public AI tools.
13. If my child is contacted unexpectedly by someone claiming to be a teacher or another trusted adult, I will encourage them to check with an adult before responding.

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent/guardian: _____

Parent/guardian of: _____

Date: _____

Appendix 3: Acceptable Use Agreement – KS1

My name is _____

14. I only use devices, apps, websites and games if I am allowed to.
15. I ask for help if I am stuck or unsure.
16. I tell a trusted adult if something online makes me worried, scared, sad or confused.
17. I am kind and polite online and in person.
18. I know that people online are not always who they say they are.
19. I know that things I see online are not always true.
20. I do not keep secrets from my trusted adults, except nice surprises such as presents.
21. I do not have to do dares or challenges that make me uncomfortable.
22. I do not get changed or undress in front of a camera.
23. I ask before sharing my personal information or someone else's photograph or story.
24. I tell an adult if I see something that is rude, frightening or not right.
25. I keep my passwords private and ask an adult if I forget them.
26. I treat people with respect whether I am using a device or speaking face to face.

My trusted adults are:

At school: _____

At home: _____

Other: _____

Appendix 4: Acceptable Use Agreement – KS2

These statements help keep me and others safe and happy at school and at home.

27. I use school devices, internet access and accounts for the purposes I have been given them for.
28. I behave online as I would face to face in the classroom.
29. I ask permission before using new devices, apps, sites or games.
30. I keep passwords private and tell an adult if I think someone knows mine.
31. I do not click unexpected links or download files unless I know they are safe and permitted.
32. I am a good friend online and do not post or share things designed to hurt another person.
33. I tell a trusted adult if I see bullying, threats, discrimination or harmful content.
34. I know it is not my fault if someone sends me something inappropriate. I do not forward it; I tell an adult.
35. I know online friends may not be who they say they are.
36. I never arrange to meet an online contact without a parent/carer or trusted adult knowing and agreeing.
37. I do not share my address, phone number, school details, passwords or live location without appropriate adult permission.
38. I think carefully before posting because online content can be copied and may remain available.
39. I follow age restrictions and the rules of apps, games and websites.
40. I do not record or photograph people without appropriate permission.
41. I do not share images of myself or others that are private, sexual or could cause harm.
42. I do not take part in dares, challenges or requests that make me uncomfortable or unsafe.
43. I use AI only when my teacher or parent/carer says it is appropriate.
44. I do not put personal information into AI tools.
45. I check AI answers because AI can be wrong, biased or misleading.
46. I do not pretend AI-generated work is entirely my own when my teacher has asked me to acknowledge AI use.
47. I respect copyright and other people's work.
48. I use safe search tools and check information before believing or sharing it.
49. I ask a trusted adult if I am unsure about anything online.

Trusted adult at school: _____

Trusted adult at home: _____

Signed: _____ Date: _____

Appendix 5: Acceptable Use Policy for Staff/Governors/Visitors & Contractors

All adults using school technology or working with pupils are expected to model safe, professional and respectful digital behaviour.

50. I understand that activity on school devices, networks, platforms and accounts may be subject to filtering and monitoring.
51. I will use school technology only for authorised purposes.
52. I will not attempt to access pupil or staff data unless I am authorised to do so.
53. I will protect my username, password and authentication information.
54. I will not make private or inappropriate contact with pupils.
55. I will not arrange meetings, tutoring or communication with pupils outside approved school processes.
56. I will not photograph, film or record pupils or school activities using personal devices unless expressly authorised.
57. I will protect confidential information and comply with data protection requirements.
58. I will not upload school or pupil information to unapproved AI tools or other online services.
59. I will report safeguarding concerns, inappropriate behaviour, lost devices, phishing, suspected cyber attacks and data breaches promptly.
60. I understand that inappropriate or unlawful use may lead to removal of access, safeguarding action, disciplinary action or termination of a contract/visit.

I have read, understood and agreed to this policy.

Signature: _____

Name: _____

Organisation: _____

Visiting / accompanied by: _____

Date / time: _____

Appendix 6: Glossary of cyber security terminology

Term	Definition
Antivirus / anti-malware	Software and services designed to identify, block or remove malicious software.
Backup	A separate copy of data that can be used to restore information after loss, corruption or a cyber attack.
Breach	Unauthorised access to, disclosure of, alteration to or loss of information, systems or services.
Cloud	Online services that provide access to data, software or computing resources over the internet.
Cyber attack	A deliberate attempt to access, damage, disrupt or misuse computer systems, networks or data.
Cyber incident	An event that affects or may affect the confidentiality, integrity or availability of information or systems.
Cyber security	Measures used to protect devices, services, networks and information from attack, damage or unauthorised access.
Firewall	A security control that manages network traffic according to defined rules.
Malware	Malicious software including viruses, trojans, spyware and ransomware.
MFA	Multi-factor authentication. Using two or more different factors to verify a user's identity.
Patching	Applying software or firmware updates, often to fix security vulnerabilities.
Phishing	A deceptive message designed to trick someone into revealing information, clicking a malicious link or taking another harmful action.
Ransomware	Malicious software that prevents access to systems or data, often by encrypting files and demanding payment.
Social engineering	Manipulating people into revealing information or taking an action that benefits an attacker.
Spear-phishing	A targeted phishing attack designed for a particular person or organisation.
Trojan	Malicious software disguised as legitimate software or a useful file.
VPN	Virtual private network. A technology that can provide an encrypted connection between a device and a network or service.
Whaling	A highly targeted phishing attack aimed at a senior or influential person.
Generative AI	AI that creates new content such as text, images, audio, video or code.
Data breach	A security incident involving accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

This policy should be reviewed against current DfE, Trust, safeguarding, data protection and cyber security requirements whenever there is a significant change to legislation, statutory guidance, technology or school practice.