Acceptable use of technology - including Use of Wi-Fi

Sussex Road Primary School

Approved by:	HT	**Date:**	September 2025
Next review due:	September 2026		

Acceptable Use of Technology for Staff, Governors, Visitors and Volunteers Staff

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Sussex Road Primary School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for pupils, they are asked to read and sign this Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Sussex Road Primary School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school/setting or accessed by me as part of my role within, professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email, data and data storage, remote learning systems and communication technologies.

2. I understand that Sussex Road Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school Child Protection Policy and Staff Code of Conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of school devices and systems

4. I will only use the equipment and internet services provided to me by the school, for example school provided laptops, tablets, and internet access, when working with pupils.

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed; this use at the school's discretion and can be revoked at any time.

Data and system security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

- I will use a 'strong' password to access school/setting systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.
- I will protect the devices in my care from unapproved access or theft.

8. I will respect school's system security and will not disclose my password or security information to others.

9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to ICT Network Services (Brian Clark).

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT Network Services.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the school's information security policies.

- All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
- Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the school Data Protection Officer and leadership team prior to use to ensure it is safe and legal.

12. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. I will only use the school's password protected Microsoft 365 Account to upload any work documents and files in a secure environment or the school setting.

13. I will not store any personal information on the school IT system, including school laptops or similar devices issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

14. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences:

- to gain unauthorised access to computer material
- to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

15. I will not attempt to bypass any filtering and/or security systems put in place by the school.

16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to ICT Network Services Ltd as soon as possible.

17. If I have lost any school-related electronic documents or files, I will immediately report this to the ICT Network Services Ltd, Self Report a potential data breach using GDPRiS and advise the Headteacher.

18. I understand images of pupils must always be appropriate and should only be taken with school provided equipment and only be taken/published where pupils parent/carer has given explicit written consent. This consent is recorded on Arbor

Classroom practice

19. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Sussex Road Primary School as detailed in the Child

Protection Policy, and as discussed with me as part of my induction and ongoing safeguarding and child protection staff training.

20. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider, in line with the school Child Protection Policy.

21. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the Child Protection Policy.

22.I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, its use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:

- AI tools are only to be used responsibly and ethically, and in line with our school Child Protection, Data Protection, and Staff Code of Conduct.
- I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
- AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving pupils.
- Only approved AI platforms may be used with pupils. Pupils must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- Any misuse of AI will be responded to in line with relevant school policies, including but not limited to the, Anti-Bullying, Staff Code of Conduct and Child Protection policies.

23. I will promote online safety with the children pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:

- exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
- creating a safe environment where children pupils feel comfortable to report concerns and saying what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
- involving the Designated Safeguarding Lead (DSL) (Sarah Miles) or a deputy as part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
- Informing the DSL or Deputy DSLs if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
- make informed decisions to ensure any online safety resources used with pupils is appropriate.

24. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile devices and smart technology

25. I have read and understood the school's Mobile Phone and Smart Technology Policy which addresses use by both pupils and staff.

26. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the Staff Code of Conduct and the school Mobile Phone and Smart Technology Policy.

Online communication, including use of social media

27. I will ensure that my use of communication technology, including use of social media, is compatible with my professional role, does not interfere with my work duties and takes place in line with the Child Protection Policy and Staff Code of Conduct.

28. As outlined in the Staff Code of Conduct:

- I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
- I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.

29. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

- I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.
- I will not share any personal contact information or details - such as my personal email address or phone number - with pupils.
- I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
- If I am approached online by a current or past pupil or parent/carer, I will not respond and will report the communication to the Headteacher (DSL) or Deputy DSLs.
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL or Deputy DSLs

Policy concerns

30. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act. 29

31. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

32. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

33. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the school child protection policy.

34. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school Child Protection Policy and/or the Allegations Against Staff Policy.

Policy Compliance and Breaches

35. If I have any queries or questions regarding safe and professional practice online, either in school or off site, I will raise them with the DSL or Deputy DSLs.

36. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

37. I understand that if the school believes that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the Staff Code of Conduct.

38. I understand that if the school believes that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the Staff Code of Conduct.

39. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Sussex Road Primary School's Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Wi-Fi Acceptable Use Policy

1. The school provides Wi-Fi for the school community. For school provided devices Networks and passwords can be obtained from the School Office, where the user's details will be logged for monitoring purposes. Staff wising to add personal devices to the network must submit their details and device IP address to ICT Network Services to enable access and monitoring. An independent guest network is enabled in school for governor use only. Access must be requested from ICT Network Services.

2. I am aware that the school will not be liable for any damage or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.

3. The use of technology falls under Acceptable Use of Technology Policy (AUP), Mobile Phone and Smart Technology Policy and Child Protection Policy which all pupils, staff, visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences to:

- gain unauthorised access to computer material
- to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6. I will take all practical steps necessary to make sure that any equipment connected to the school's service is adequately secure, such as up-to-date anti-virus software, and system updates.

7. The school cannot guarantee the safety of traffic across its wireless service. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security and will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10.I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

11.My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP, the law (including copyright) and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and other devices or websites.

12.I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

13.I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the DSL as soon as possible.

14.If I have any queries or questions regarding safe behaviour online, I will discuss them with DSL or Deputy DSLs.

15.I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

Appendix A

Pupil Acceptable Use of Technology

Early Years and Key Stage 1 (0-6)

• I understand that the school/setting rules will help keep me safe and happy when I go online.

• I only go online when an adult is with me.

• I only click on online things online when I know what they do. If I am not sure, I ask an adult first.

• I keep my personal information and passwords safe.

• I only send polite and friendly messages online.

• I know the school can see what I am doing online when I use school computers/tablets.

• If I see something online that makes me feel upset, unhappy, or worried I will always tell an adult.

• I can visit www.ceopeducation.co.uk to learn more about keeping safe online.

• I know that if I do not follow the school rules there may be a consequence

• I have read and talked about these rules with my parents/carers.

Key Stage 2

I understand that the school's Acceptable Use Policy will help keep me safe and happy online at home and at school.

Safe.

• I will be kind and respectful online, just like I am in school.

• I only send messages which are polite and friendly.

• I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.

• I will only click on links if a trusted adult says they are safe.

• I know that people online might not be who they say they are. I will only chat with people I know or who a trusted adult says are safe.

• If someone online asks to meet me, I will tell a trusted adult straight away.

Learning

• I always ask permission from an adult before using the internet.

• I only use websites, tools and/or search engines that my teacher has chosen or given me permission to use.

• I use school devices for schoolwork unless I have permission otherwise.

• If I need to learn online at home, I will follow the same rules that I do at school.

Trust

• I know that some things or people online might not be honest or truthful.

• If I'm not sure if something online is true, I will check with other websites, books, or ask a trusted adult.

• I always credit the person or source that created any work, images, or text I use.

• I will use Artificial Intelligence (AI) tools safely and sensibly. I won't use them to cheat, copy other people's work, or say anything unkind. I know that AI tools can sometimes make mistakes. I will only use them when a teacher or trusted adult says it's okay.

Responsible

• I keep my personal information safe and private online.

• I will keep my passwords safe and will not share them.

• I will not access or change other people's files or information.

• I will only change the settings on a device if a member of staff has allowed me to.

Tell

• If I see anything online that makes me feel worried or upset, I will tell an adult, minimize the screen, or turn off the screen and tell an adult immediately.

• If I am aware of anyone being unsafe with technology, I will report it to a teacher/adult at school/setting.

• I know it is not my fault if I see something upsetting or unkind online.

• If I'm not sure about something online or it makes me feel worried or scared, I will talk to a trusted adult.

Understand

• I understand that the school internet filter is there to protect me, and I will not try to bypass it.

• I know that all school owned devices and networks are checked/monitored to help keep me safe, even if I use them at home. This means someone at the school may be able to see and/or check my online activity when I use school devices and/or networks if they are worried about my or anyone else's safety or behaviour.

• I have read and talked about these rules with my parents/carers.

• I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to see help.

• I know that if I do not follow the school Values then there may be a consequence.

Appendix B

Acceptable Use of Technology for Parents/Carers

1. I have read and discussed Pupil Acceptable Use of Technology Policy (AUP) with my child and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child's use of school devices and personal use where there are safeguarding and/or behaviour concerns. This may include where online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I understand that any use of school devices and systems are appropriately filtered. Further information can be found on the Filtering and Monitoring page on the school website.

4. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons. Monitoring approaches are in place to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.

6. I am aware that the school Mobile Phone and Smart Technology Policy states that my child cannot have personal devices, including mobile and smart technology on site.

7. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote learning AUP.

8. My child and I are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.

9. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.

10. I will inform the school or other relevant organisations if I have concerns about my child's or other members of the school community's safety online.

11. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

12. I understand my role and responsibility in supporting the school online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.