

Capel-le-Ferne Primary School	
Acceptable Use of Technology Policy (AUP)	
Date agreed by Governors	27.09.2023
Date of next review	September 2024
Further information about policy	<p>This policy will be reviewed at least annually and/or following any updates to national and local guidance and procedures.</p> <p>The policy is written using latest KCC template.</p> <p>The policy is adapted from KCC/TEP model policy.</p>
<p>"Learning today for life tomorrow"</p> <p>Our Values: Independence, Creativity, Confidence, Respect</p>	
<p>This policy applies to pupils attending Capel-le-Ferne Primary School and parents/carers.</p>	



This is a core policy that forms part of the induction for all staff. It is a requirement that all members of staff have access to this policy and sign to say they have read and understood its contents.

Learner Acceptable Use of Technology Statements:

Early Years and Key Stage 1 (0-6)

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

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers and tablets.
- I always tell an adult/teacher/member of staff if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules:
 - The relationship and behaviour policy will be followed – possibly resulting in the school contacting parents directly, depending upon the severity of the offence.

Further details are outlined in the school's relationship and behaviour policy and Keeping children Safe in Education 2023.

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

Key Stage 2 (7-11)

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

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with and open messages from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- I understand that personal devices are not allowed to be used within the school setting.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school devices for school work.
- If I need to learn online at home, I will follow the school remote learning AUP.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

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.

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 devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that I will be able to use the internet in school for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.

- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidentally come across any of these I should report it to a teacher or adult in school, or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my school name or by sending a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I know it is not my fault if I see or someone sends me something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

Acceptable Use of Technology Statements and Forms for Parents/Carers

Parent/Carer AUP Acknowledgement

Capel-le-Ferne Primary School Learner Acceptable Use of Technology Policy Acknowledgment

1. I, with my child, have read and discussed Capel-le-Ferne Primary School learner acceptable use of technology policy (AUP) and understand that the AUP will help keep my child safe online.
2. I understand that the AUP applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.
3. I am aware that any use of school devices and systems may be monitored for safety and security reason 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.
4. I am aware that the school mobile phone policy states that my child cannot use personal device and mobile technology on site. Mobile phones must be switched off and handed to the office at the beginning of the day. These will remain switched off until the end of the school day. Only children who require a mobile phone for one of the outlined reasons will be permitted to bring one into school.
5. I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised.
6. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.
7. I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
8. 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.
9. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.
10. 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.

11. I will support the school online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Agreement with this policy is an expectation of all parents/carers who choose to send their child for their education to Capel-le-Ferne Primary School.

Child's Name.....

Class..... Date.....

Parent Name.....

Parent Signature..... Date.....

Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Capel-le-Ferne 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 learners, they are asked to read and sign that they have read, understood and will comply with the Staff 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 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.

This policy outlines the staff roles and responsibilities linked to filtering and monitoring as set out in KCSIE 2023.

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within school both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.
2. I understand that school Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school 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, mobile phones, and internet access, when working with learners.
5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is not allowed.

6. Where I deliver or support remote learning, I will comply with guidance provided by the school in the Remote Learning AUP.

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 systems. A strong password has numbers, letters and symbols, with 8 or more characters and is only used on one system.
- I will protect the devices in my care from unapproved access or theft. Do not leave devices visible or unsupervised in public places.

8. I will respect school 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 the IT system manager.

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school 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 removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school. All memory sticks and portable hard drives must be password protected.

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. Where possible, I will use Microsoft SharePoint to access documents outside of school.

13. I will not store any personal information on the school IT system, including school laptops or similar device 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 Primary Technologies as soon as possible.

17. If I have lost any school related documents or files, I will report this to the Headteacher (Anthony Richards) who will then seek assistance through the ICT Support Provider (Primary Technologies) and the school Data Protection Officer (DPO: Accordio Ltd) as soon as possible.

18. Any images or videos of learners will only be collected on school based files and storage areas. They will only be published per permissions collected.

- I understand images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

19. I am aware of the expectations relating to safe technology use in the classroom, and other working spaces.

20. I have read and understood the school mobile phone policy and online safety policy.

21. I will promote online safety with the learners 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 learners feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
- involving the Designated Safeguarding Lead (DSL) (name) or a deputy (names) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with learners is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school child protection policies.

23. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Use of Social Media and Mobile Technology

24. I have read and understood the school policy which covers expectations regarding staff use of mobile technology and social media.

25. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff behaviour policy, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.

- I will take appropriate steps to protect myself online when using social media as outlined in the [social media policy](#).
- I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the [mobile technology policy](#).
- I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
- I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school/setting behaviour policy/code of conduct and the law.

26. My electronic communications with current and past learners 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 with learners, such as my personal email address or phone number.
- I will not add or accept friend requests or communications on personal social media with current or past learners and/or parents/carers.
- If I am approached online by a learner or parents/carer, I will not respond and will report the communication to my line manager and a Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or headteacher

27. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the DSL and/or the headteacher.

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

30. 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.

Policy Compliance

31. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

Policy Breaches or Concerns

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

33. I will report concerns about the welfare, safety, or behaviour of staff to the headteacher, in line with the allegations against staff policy.

34. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.

35. I understand that if the school believe 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 behaviour policy/code of conduct.

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

Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology.

This AUP will help Capel-le-Ferne Primary School ensure that all visitors and volunteers understand the school expectations regarding safe and responsible technology use.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within Capel-le-Ferne Primary School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies.
2. I understand that Capel-le-Ferne Primary School AUP should be read and followed in line with the school Code of Conduct.
3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all 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.

Data and Image Use

4. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.
5. I understand that I am not allowed to take images or videos of learners. Any images or videos of learners will only be taken in line with the school camera and image use policy.

Classroom Practice

6. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners.
7. Where I deliver or support remote learning, I will comply with the latest school guidance on providing remote learning.
8. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.
9. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to a Designated Safeguarding Lead (DSL) in line with the school child protection policy.

10. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.

Use of Social Media and Mobile Technology

11. I have read and understood the school policy which covers expectations regarding staff use of social media and mobile technology.

12. I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.

- I will take appropriate steps to protect myself online as outlined in the online safety/social media policy
- I will not discuss or share data or information relating to learners, staff, school/setting business or parents/carers on social media.
- I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct/behaviour policy and the law.

13. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.

- All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
- Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
- Any pre-existing relationships or situations that may compromise this will be discussed with a DSL and/or head teacher.

14. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with a Designated Safeguarding Lead and/or the headteacher.

15. 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.

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

17. 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.

Policy Compliance, Breaches or Concerns

18. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
19. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to a Designated Safeguarding Lead in line with the school child protection policy.
20. I will report concerns about the welfare, safety, or behaviour of staff to the headteacher, in line with the Whistleblowing policy.
21. I understand that if the school believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.
22. I understand that if the school suspects criminal offences have occurred, the police will be informed.