Acceptable Use Policy

Review Date: September 2025

Next review Date: September 2026

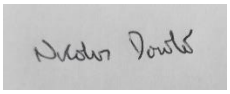
Adopted by the Governing Body on: 22nd Sept 2025

Please read this policy alongside our school Child protection and Safeguarding Policy, Code of conduct (employees), School Disciplinary Policy and Procedures, Online Safety policy and other relevant policies. This policy is cross-referenced against Annex D of KCSiE25.

Review

The governing body reviews this policy annually. The governors may, however, review the policy earlier than this, if the government introduces new regulations, or if the governing body receives recommendations on how the policy might be improved.

VERIFICATION CERTIFICATE

Document Title: Issue:	Policy 4
Reviewer: Position: Signature: Date:	Ceri Baggus Designated Safeguarding Lead  9.9.25
Approver: (on behalf of the Governing Body) Position: Signature: Date:	Nicolas Dowler Chair of Governors  22/09/25

DOCUMENT ISSUE/AMENDMENT HISTORY
(previous versions not numbered nor amendments noted)

Issue	Date	Amendment
1	4.10.22	Policy reviewed and updated for full governor
2	2.9.23	Policy reviewed and updated, as appropriate, for full Governor ratification.
3	26.8.24	Policy reviewed and updated, as appropriate, for full Governor ratification.
4	9.9.25	Policy reviewed and updated, as appropriate, for full Governor ratification. Updates are highlighted in red

Computer network

- Obtaining, downloading, sending, printing, displaying, distributing or otherwise transmitting or gaining access to materials which are pornographic, obscene, racist, unlawful, abusive, offensive or inappropriate will be regarded as gross misconduct and will result in disciplinary action.
- Distributing abusive, discriminatory or defamatory statements will be regarded as gross misconduct and will lead to disciplinary action.
- Any software that is installed must be covered by the appropriate licensing agreements.
- Copyright of materials available on the network must be respected.
- Pupils must not be allowed access to the teacher laptop within the classroom.
- No personal data about pupils or their families should be stored on memory sticks or school laptops, which are taken off site. Any photographs or documents containing personal information about pupils or their families must be stored securely on the TDrive or Google Drive, which is only accessible through each staff member's own individual password.
- School laptops must be used for professional purposes only when taken off school premises and must not be used for any personal purposes.
- All school computers must be password protected and must be logged off and shut down at the end of each school day. They must also be logged off/ locked whenever staff members are not present in the room. Sensitive websites such as G-Mail and SIMS must be logged off when not in use. Passwords for school computers will be automatically updated on a regular basis.

Internet / e-mail

- Use of GCC Internet and email must be solely for legitimate school purposes.
- Use of the internet and email are subject to scrutiny by the school's filtering provider. Any action that might damage the reputation of the school will be dealt with as a serious act of misconduct. The Designated Safeguarding Lead has responsibility for overseeing the filtering and monitoring systems and processes in place in school.
- Use of the school internet for personal financial gain, gambling, political purposes or advertising is forbidden. This includes the personal buying or selling of goods.
- You are responsible for the security of your passwords - ensure that your passwords for professional sites are different to those for personal sites and that they are not written down in full anywhere.
- E-mails sent from school should contain the same professional levels of language and content as applied to letters or other media.
- You are responsible for the email you send and for any contacts you make that might result in inappropriate emails being received.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Staff must not open any attachments to emails unless the source is known and trusted.
- Appropriate security must be used or applied before confidential or sensitive information is sent via the internet or email.
- If staff members need to communicate with pupils for work purposes they can only do so through the official school email. Personal e-mail addresses must not be shared with pupils or parents.

Use of photographs, video and digital images

- Staff must only use school equipment to record, or take photographs of pupils, and only then if the relevant permission has been obtained.
- Cameras and memory sticks containing photographs and videos must not be taken off the school site.

Phone use

- A professional tone is to be used in all phone calls made and text messages sent using work phones.
- Work phones are not to be used for personal calls, other than in an emergency.
- Calls and contact to pupils and parents should only use school telephones or school mobile telephones. Staff must not share their personal contact details.
- Direct contact with pupils by telephone calls or text messages is limited to essential service needs only.
- Personal mobile phones must never be used or be visible in the classroom, or anywhere where pupils are present. They must be stored out of sight and only used during break and lunchtimes, as long as no pupils are present.
- Any urgent phone calls which staff are expecting to receive must come through to the school office phone and a message will then be sent straight to class. They must not be taken on personal mobiles.
- Due to the accessing of work e-mails on personal mobile phones, devices must be protected by a security passcode which only the owner knows. This passcode should not be shared with even friends

or family members.

Social Media

Social Media is used increasingly across society and is recognised as a hugely valuable communication tool. However, the open nature of the internet means that social networking sites can leave professionals (such as teachers and other staff working in education) vulnerable if they fail to observe a few simple precautions.

- Staff members must not identify themselves as employees of the school in their personal web-space apart from professional websites such as LinkedIn. This is to prevent information on these sites from being linked with the school and the County Council and to safeguard the privacy of staff members.

- Staff members must not make contact through any personal IT or social medium with any pupil, whether from our school or any other school, unless the pupil is your own family member OR an existing close family friend. School does not expect staff members to discontinue contact with their own family members or significant family friends via personal social media; however care should be taken not to communicate with friends of the family member who may be school pupils.

- Staff members must decline 'friend requests' from pupils they may receive in their personal social media accounts and must not send 'friend requests' to pupils.

- Staff will exercise caution when inviting, or receiving invitations from work colleagues and family members of pupils to be 'friends' on personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships.

- Any information staff members have access to as part of their employment, including personal information about pupils and their family members and colleagues, must not be discussed on their personal web-space or social media sites.

- Photographs, videos or any other types of image of pupils and their families or images depicting staff members, who can be identified as school staff, must not be published on personal web-space or social media sites.

- School e-mail addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

- Staff members must not edit open access online encyclopedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

- School logos or brands must not be used or published on personal web-space/social media sites (apart from professional websites such as LinkedIn).

- School does not permit personal use of social media or the internet during core contracted work hours. Access to social media sites for personal reasons is not allowed between 8.35am and 3.30pm (apart from during break and lunch times). Any access to these sites during these break times must be on personal devices and not school devices. Staff members are expected to devote their contracted hours of work to their professional duties.

- Staff members must ensure that they do not post anything negative about the school on social media sites or comment on other people's negative posts regarding the school or members of staff. Staff must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals/organisations, school or the County Council. Anything of concern related to the school which you witness on social media, please report to a senior member of staff.

- Staff members are advised to set the privacy levels of their personal social media sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

BREACHES OF THE POLICY

- Any breach of this policy will be investigated and may lead to disciplinary action being taken against the staff member/s involved in line with the Staff conduct policy.

- A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the school or any illegal acts or acts that render the school or the County Council liable to third parties may result in disciplinary action or dismissal.

- Contracted providers of the school must inform the relevant service or County Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the service and the County Council. Any action against breaches should be according to contractors' internal disciplinary procedures.

If you are in doubt about any of the above, please seek advice.

Appendix1

Cirencester Primary School Acceptable Use Agreement All Staff / Governors and Visitors.

1. I have read and understood Cirencester Primary's full Online Safety and Acceptable Use policies and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
3. I understand the responsibilities listed for my role in the school's Online Safety and Acceptable Use policy. This includes promoting online safety as part of a whole school approach in line with the **RSHE curriculum,** as well as safeguarding considerations when supporting pupils remotely.
4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, by:
    - not sharing other's images or details without permission
    - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Acceptable Use Policies. I will report any breach of this by others or attempts by pupils to do the same to the headteacher. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety and Acceptable Use policies. If I am not sure if I am allowed to do something in or related to school, I will not do it and seek guidance from the DSL.
7. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either.
8. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords. I will only use complex passwords and not use the same password as for other systems.
9. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
10. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
11. I understand and support the commitments made by pupils/students, parents and fellow staff, Governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
12. I will follow the guidance in the safeguarding and online-safety policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment and misuse of technology

13. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

Declaration by the user

As part of our annual sharing of school safeguarding policies, I will sign the self-declaration form to say that I have read, understood and agreed to the Online Safety and Acceptable Use policies. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Appendix 2

All Staff at Cirencester Primary School – Staff Proxy Internet Unfiltered Service Agreement – To be signed when joining the school and then as part of annual safeguarding self-declaration form.

"You must not leave your browser session open when your computer/ laptop is left either unattended or unlocked"

South West Grid for Learning (SWGfL)

The aim of this agreement is to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk.

The SWGfL encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise the SWGfL's information and computer systems.

The agreement applies to all staff at Cirencester Primary School who use the Staff Proxy Unfiltered Service to assess sites such as You Tube, Facebook, Twitter and any linked sites.

Use of Internet facilities

For the purposes of this agreement, Internet usage means any device with a connection to the Internet via Web browsing, email or newsgroups (public discussion groups) or other software.

Staff Proxy

Unfiltered proxy service is to allow access to certain sites (in which parts may be deemed safe for use as teaching resources but may still not be safe for pupil access) which would normally be blocked. However, this now requires a username and password to access the service which is linked to your computer login and no one else should be given access to your computer login.

Passwords are issued on a per user basis and Staff need to keep this password safe and not share with anyone else. In order to use the Staff Proxy service, you must agree and abide to the Acceptable Use Policy above, and the following conditions in this agreement: -

- All internet usage will be logged against your username and that you are subject to the above Acceptable Use Agreement terms andconditions.
- Any inappropriate web access/misuse of this service may cause your access to be revoked and action taken againstyou.

You must not leave your browser session open when your computer/ laptop is left either unattended or unlocked as unauthorised users (i.e. Pupils or Parents) may get brief access to this service which would count as misuse and may also cause this service to be revoked form you and or the school.

Therefore you must either close your session of Internet Explorer, or if not you must lock your computer before leaving it unattended.

SWGFL - Monitoring and Access

If inappropriate material is accessed accidentally, staff should immediately report this to the Headteacher, who will then report to SWGfL, so that this can be taken into account in monitoring. SWGfL acknowledges that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use (for example investigating racial issues). Any such access should be pre-planned and recorded so that it can be justified if required.

SWGfL will monitor and audit the use of the Internet to see whether users are complying with the agreement. Any potential misuse identified by the SWGfL will be reported to the school. On

evidence provided by the SWGfL, a member of staff may be disciplined by their employer. At the same time, if a user's conduct and/or action(s) are illegal, the member of staff may become personally liable in some circumstances.

All Staff at Cirencester Primary School – Staff Proxy Internet Unfiltered Service Agreement

I agree to follow the Staff Proxy Internet Unfiltered Service Agreement and

I agree not to leave my browser session open when my computer/ laptop is left either unattended or unlocked.

User Full Name.....(printed)

Job title ……

User Signature ……..……..…