Acceptable Use of Technology

All Staff, Governors, Visitors and Volunteers Agreement Form

Date of Agreement: 28/09/26
Policy Reviewed by: Dan Williamson
Date of Next Review: September 2027

This guidance and agreement has been written to ensure all members and visitors of Castle Camps Primary School are kept safe and use appropriately all digital technologies in school. The term digital technologies covers: access to the internet, use of e-mail and other communication tools, use of the school intranet, network resources, and any form of software and electronic hardware inclusive of mobile phones.

Use of the Internet and E-mail

- All use of the internet at school should be primarily to enhance teaching and learning or for administrative use, although it is understood that staff may occasionally need to use the internet for personal reasons. Any personal use, however, must never take place when supervising or responsible for children in the school.

- Internet access in school is regularly monitored. Both County and school-based filtering systems are in operation for both staff and pupils and are set at an appropriate level of limitation to safeguard against inappropriate content. This includes the blocking of all generative AI software at the pupil level.

- All staff who have a computer allocated to them have an Outlook school e-mail address, which is accessible through a web browser. Use of this school e-mail address is for all correspondence related to the school and should be used for no other purpose.

- The accessing of inappropriate and indecent materials from the internet or via e-mail is prohibited and may result in disciplinary action being taken.

Personal email accounts

Staff use of personal email for school business is prohibited and subject to the school's disciplinary procedures. Unregulated communication can put individual members of staff and the school at risk of prosecution. School business includes (but is not limited to) communication with pupils, parents, governors, other members of staff and third parties such as suppliers of school equipment or government agencies. For this reason, auto-forwarding of email to external accounts is disabled and staff must make themselves aware of the risks posed by forwarding any email externally. We also ask the Governing Body adopts the same principle for their own communications.

Use of ICT hardware and software

- Each member of staff has a unique login for the network via hardware that has been administered by the school. Passwords must be strong (using a mix of different words, characters, and cases), unique and not shared with anyone. Staff must immediately change their password if they believe it has been compromised. Multi-factor authentication will be used to protect access to school systems where appropriate. Passwords should not be divulged to anyone else unless deemed necessary by the Headteacher. It is also recommended that staff adopt the best practice of combining random words and including at least one number and special character.
- Software that allows access to sensitive data such as Email and Google Classroom, BromCom and MyConcern must be protected with two-factor authentication through the Microsoft Authenticator App. This will be enforced by the school. Access to particular drives is controlled and granted by the Headteacher as stated in the school's cyber security policy.
- When using any IT equipment with pupils you are expected to be in the room at all times and are responsible for ensuring that use of hardware and software by pupils is appropriate and safe. The school will put necessary safeguards in place to ensure that this is the case but it is for staff to use only software and hardware that is affiliated with the school.
- It is the responsibility of all staff to ensure that pupils do not have access to confidential data (such as MIS BromCom) and must therefore be vigilant in their security measures. In particular, staff must ensure their laptop is locked when left unattended and that whiteboards that are connected to laptops are off or 'frozen' when checking emails or using software that contains confidential information.
- All software that is installed locally on school devices needs to be approved by the Headteacher. This is to prevent a compromise to the network (including bypassing filtering and security systems) or the installation of software that is not adequately licensed.

Cyber Security

Any suspected cyber security incident, including phishing emails, malware infections, accidental disclosure of personal data, compromised accounts, or any suspicious activity on school systems, must be reported immediately to the Headteacher and/or the school's IT support provider. Further information on how this is monitored and the school's IT infrastructure is protected can be found in our Cyber Security Policy.

Use of AI Tools

Staff may only use AI systems that have been approved by the school. Personally identifiable pupil data, staff data, safeguarding information or other confidential school information must not be entered into AI systems unless specifically authorised and covered by appropriate data protection arrangements.

Child Protection

- Whilst access to unsuitable internet content is minimised by NetSweeper (our filtering software), this can never be completely eliminated. It is therefore important that staff recognise their duty of care to ensure that pupils do not actively try to access or search for inappropriate website content.
- In addition, pupils should not give out personal information online and, through our curriculum, will be taught what is appropriate to share when using online and safe digital practices through our PSHE lessons.
- If you suspect that illegal content has been accessed on a computer, the workstation should be immediately secured and bring the device to a member of SLT.
- Additional guidance on online safety is contained in the Safeguarding and Child Protection Policy and Cyber Security Policy.

Staff Personal Mobile Phone Policy Statement

Use of mobile phones
Staff members are permitted to bring personal mobile phones onto school premises for essential personal use and emergency contact only. Staff may make or receive urgent personal calls or check personal notifications only under the following strict conditions:

- **Location & Presence:** It is the individual staff member's responsibility to ensure that they use a personal mobile device in a room vacant of children, unless in an emargency. The use of designated, adult-only areas - specifically the Staffroom - is strongly recommended.
- **Storage:** When not in permitted use, personal mobile phones must be switched off or placed on silent and stored securely out of sight (e.g., in a locked drawer, locker, or bag).
- **Staff Permitted Use:** To maintain a secure, professional, and phone-free environment for pupils, personal devices must be kept on silent and out of sight of pupils. Staff must never use personal devices to contact pupils, parents, or carers under any circumstances. Mobile phones **must not be visible or used in the presence of pupils** at any point during the school day.
- **Appropriate Content & Conduct:** Staff must ensure personal devices contain no illegal or inappropriate material. Sending inappropriate messages and recording images or audio of any member of the school community without prior consent are strictly forbidden.
- **Liability:** The school accepts no responsibility or liability for the loss, damage, or theft of any personal mobile device on school premises.

Cyber Security & Network Safeguarding Compliance
In alignment with Department for Education (DfE) Cyber Security Standards and data protection requirements:

- **Network Access:** Personal mobile devices must never be connected to the school's Wi-Fi network, internal servers, or admin systems. Where internet access is required, staff must use either their own cellular data.
- **Authentication Security:** Personal mobile phones used to generate Multi-Factor Authentication (MFA) codes or run authenticator apps for school accounts must be protected by a strong passcode, PIN, or biometric lock (Face ID/Fingerprint).
- **Passcode Security:** Staff must secure all personal devices with a strong, non-predictable PIN or passcode (minimum 6 digits or alphanumeric is recommended) and enable an automatic screen lock after a brief period of inactivity.
- **Data Protection & Media:** Under no circumstances should personal mobile phones be used to capture, store, or transmit photographs, video, audio, or personal data of pupils or staff. Personal devices must not be used to access confidential school systems or data, including emails unless approved by the Headteacher.
- **Incidents:** Any suspected loss, theft, or cyber security compromise of a personal device that holds school-related authenticators or data must be reported immediately to the IT Lead (Dan Williamson) or Headteacher.

Castle Camps C of E Primary School

Acceptable Use of Technology Declaration

I have read through the 'Acceptable Use of Technology Agreement' and agree to the expectations and to those specifically stated below:

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I understand that personal devices will not be granted access to the school's network, and this can only be accessed through a trusted school device. Exceptions to this are stated in the school's e-safety and cyber security policy.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access e-mail / internet / intranet / network or other school systems I have access to through school devices.
- I will ensure all documents, data etc, are printed, saved, accessed and deleted / shredded in accordance with the school's data security policy.
- I will not engage in any online activity that may compromise my professional responsibilities which includes the use of social media.
- I will only use the school approved e-mail system(s) for any school business, including communication with parents. I will only enter into communication regarding appropriate school business.
- I will only use the school's approved systems and school network to communicate with pupils, and will only do so for teaching and learning purposes.
- I will not browse, download or send material that could be considered offensive to colleagues or others.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to the IT lead or Headteacher.
- I will not download any software or resources from the internet that are not approved by the Headteacher.
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author's permission.
- I will not connect any device (including USB flash drives) to the network that has not been approved by the Headteacher.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home on personal equipment. If this is required, such as a residential trip, then this must be first approved by the Headteacher.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the school approved system and/or equipment.
- I will follow the school's policy on use of mobile phones / devices at school.

- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with or compromise my professional role.
- I agree and accept that any hardware loaned to me by the school is provided solely to support my professional responsibilities, and that I will notify the school of any "significant personal use", as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is password protected, and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information that is held within the school's information management system will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the school's child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand any loss or theft of a school device must be reported immediately to the Headteacher and/or the school's IT support provider.
- I understand that all internet usage and network usage can be logged, and that this information can be made available *to the Headteacher* / *Safeguarding Lead* on their request.
- *All teaching and support staff:* will embed the school's e-safety / digital literacy curriculum into their teaching and learning role.

Acceptable Use Agreement Form: Staff, Volunteers, Visitors, Governors

User Signature

I agree to abide by all the points in the Acceptable Use of Technology Agreement.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to remain up to date with the school's current Safeguarding and Child Protection, Acceptable Use of Technology, Cyber Security and Data Protection policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature……Date..... Full Name… (printed)

Job Title / Role… (printed)

I approve this user to be set-up on the school systems relevant to their role.

Authorised Signature (Headteacher)……..