Learning, to make a difference, in God's world

Pilgrims' Cross CE Aided Primary School

Acceptable Use of Technology

(includes e-safety and social media policies)

PILGRIMS' CROSS CE AIDED PRIMARY SCHOOL

Acceptable Use of Technology

(includes e-safety and social media policies)

Acceptable Use of Technology Policy

Revision Record

Revision No.	Date Issued	Prepared By	Approved	Comments
1	October 2025	JC	FGB	Revision record added. Added clearer guidance on Year 6 use of phones- not within school grounds.
2	October 2026	JC	FGB	References to *Mobile Phones & Tech. Policy* added. Added point on filtering & monitoring. Removal of bullet point regarding school text service (no longer in use). Added point about pupil pictures on website.

All the Governors and Staff at Pilgrims' Cross CE Aided Primary School are committed to sharing a common objective to help keep the children and staff of the school safe. We ensure that consistent effective safeguarding procedures are in place in order to support the families, children and staff of the school.
This policy is inclusive of this commitment.

By ensuring our staff and children are safe online we demonstrate and focusses on the school's value. Staff and other adults working with pupils show Love in the care and vigilance they take to ensure the pupils stay safe online. They also show this in the way they model and teach the pupils to be respectful and responsible towards other in their use of technology. Courage is demonstrated in promoting the positive uses of technology and the learning benefits it can bring & Trust in that they will be responsible in recognising where good choices need to be made.

Cyber Ambassadors: The school has both adult and child Cyber Ambassadors so that there is a constant focus on safer learning for the children.

This policy should be read alongside our Mobile Phone & Tech Policy, Child Protection & Safeguarding Policies. It combines e-safety, acceptable use and social networking and it considers the use of both the fixed and mobile internet, PCs, laptops/netbooks/iPads/tablets, webcams, digital video equipment, mobile phones, camera phones and portable media players. The following applies not only to work and use of school ICT equipment in school, also applies to use of school ICT systems and equipment out of school and use of personal equipment in school or in situations related to my employment by the school.

Acceptable Use of Technology

(includes e-safety and social media policies)

Use the technology:

- Do not disclose username or password to anyone else, nor try to use any other person's username and password.
- Do not access, copy, remove or otherwise alter any other user's or pupil's files, without their express permission.
- Do not use any personal equipment (e.g. mobile phone cameras or smart watches) to record images, unless permission of the Head Teacher has been granted.
- Where images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured, unless parental permission has been granted.
- Do not open attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Ensure that data is regularly saved onto the network.
- Do not try to upload, download or access any materials that are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate, or may cause harm or distress to others. Do not try to use any programmes or software that allows the bypassing of the filtering / security systems in place to prevent access to such materials.
- Do not make large downloads or uploads that will take up internet capacity and prevent other users from being able to carry out their work, unless permission is given.
- Do not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor try to alter computer settings, without the permission of the Head Teacher.
- Do not cause any damage to school equipment, or the equipment belonging to others.
- Understand that data protection policy requires that any staff or pupil data to which staff have access, will be kept private and confidential, except when it is deemed necessary that staff are required by law or by school policy to disclose such information to an appropriate authority i.e. Children's Services – Child Protection
- Immediately report any damage or faults involving equipment or software, however this may have happened.
- Ensure that staff have permission to use original work of others in own work.
- Where work is protected by copyright, do not download or distribute copies (including music and videos).

Using the **internet** safely:

- Provide the children with quality internet experiences as part of their learning.
- Children will not be able to access the internet unsupervised
- The internet is filtered by the internet provider – at this time Hampshire County Council (Drift IT Services)
- Teachers will check all internet sites that they are guiding the children to use before allowing the children access
- Teachers will allow children to search the internet in a guided group only (i.e. an adult in close supervision)
- The children will be taught what is appropriate internet content and how to report anything that is not appropriate.
- Any inappropriate content will be report to the school office and a member of the admin team will inform the internet provider and request the site to be filtered.
- No access to social networking sites, use of mobile phones during teaching / supervision time by adults or children.
- The school will share advice to parents about safe internet use at home with parents on a regular basis.
- Filtering and monitoring reports produced by the school's software will be regularly checked by the Head Teacher and followed up as necessary. Governors will also monitor Filtering & Monitoring regularly.

Using **email** safely:

- Staff will only use their school email account to send messages about school business – this system is hosted by Hampshire County Council and is secure.
- The children will only be taught how to use emails using an approved email programme, approved by the Head Teacher
- No personal information will be shared via email
- Any email received that is deemed to be inappropriate should be reported to the Head Teacher at once.

Using **social networking**:

- The use of online chat rooms, instant messaging services and text messaging is not permitted during school hours by adults or children.
- No personal information is shared via social networking
- No member of staff should interact with any pupil in the school on social networking sites.
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18.
- No member of staff should post anything on their own social networking site whilst at work or undertaking duties relating to the care of the pupils (e.g. residential trips, visits etc.)
- No member of staff should post anything about the school or respond to anything posted by anyone else about the school.
- If you have any evidence of pupils or adults using social networking sites inappropriately, please contact the Head Teacher immediately.
- It is strongly advised that staff are not friends with any parents (unless family members or friends prior to appointment) associated with the school on social networking sites. Those who do, do so at their own risk as any public contact that could be deemed as defamatory, embarrassing or bringing the school into disrepute may result in disciplinary action and may result in termination of contract.
- If a staff member is threatened by a parent or is subject to comment that may be deemed defamatory, the Head Teacher is to be informed directly – the individual should not respond directly over the social networking site. If possible the comment should be printed as a permanent record.
- If staff are made aware of any negative attention being given to the school e.g. parents' petitions, Facebook campaigns, they should immediately report this to the Head Teacher.
- The school will share advice to parents about safe internet use at home with parents on a regular basis.

School social media:

- The school's/Friends of Pilgrims' School (FOPS) Facebook page is managed by the admin team, a delegated member of FOPS, in conjunction with the IT Leader and a member of the Governing Body
- All personal information, including names and photos of pupils will only be published with specific and informed parental consent. In general, the less that can be shared, the safer the post.
- Any staff uploads to the school website must be agreed with the Head Teacher. The school website may also centrally host any online communications between staff and pupils (e.g. to support home learning tasks)

Use of **mobile phones**:

- Children are not permitted to have mobile phones on in school.
- Children are not allowed to bring smartphones onto the school premises. If their parents/carers wish for them to have a mobile phone in school (Year 6 pupils may walk to and from school with a phone, but this is not to be

used within the school grounds, it to be handed in to the class teacher immediately, upon entering the classroom & is kept secure until the end of the school day), it is to be a 'brick' or 'dumbphone'.

- Staff are not permitted to use their mobile phone or have their phones on during times when they are teaching or supervising children, unless specific permission has been granted by the Head Teacher.
- Staff will not give out their personal mobile phone numbers to children or parents.

School website:

- The school website is maintained and kept up to date by the Head Teacher and the Admin Office.
- The Head Teacher ensures that the content on the school website is accurate and appropriate to the needs of the school community.
- No personal information about any member of the school community beyond a name and photo, will be published on the website.
- Written permission from parents or carers will be obtained before photographs of pupils or pupil names are published on the website. This is done on induction. Photos will be of the backs of pupils' heads, due to recent national safeguarding concerns about deepfake images.
- No content will be uploaded onto the website unless it is agreed by the Head Teacher.

Cyber bullying:

- Cyber bullying is when the Internet, mobile phones or electronic devices are used intentionally to hurt or embarrass another person. As with any other type of bullying, Cyber bullying only occurs if a person is repeatedly tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another person using digital technology.
- Cyber Bullying will not be tolerated by the school and this will be managed by following the school's Anti-Bullying Policy.

Reporting Concerns:

- Any issues relating to staff misuse of the internet must be referred to the Head Teacher or Chair of Governors if the concern is the Head Teacher.
- Any illegal, inappropriate or harmful material or incident that staff become aware of will be report to the Head Teacher. In the case where the Head Teacher is the alleged perpetrator, staff will report to the Chair of Governors.
- **All staff will maintain high standards of ethics and behaviour, within and outside school and this includes when on the internet and using social media.**
- If staff comment or "like" any statement seen on the internet and social media, they must be aware that their comments will be viewed "as a member of staff or governor." This applies to private and personal communications.
- Staff will not share any negative opinions of the school, governors, parents/carers or children on the internet, including social media. If they have any concerns about another staff member's online behaviour, then they must share these with the Head teacher or the Chair of Governors.
- Staff should report, to the Head teacher, any negative comments seen on the internet or social media about any member of staff or the school or which suggest any type of aggressive behaviour towards any member of the school community. Staff will not comment online to these types of comments, positively or negatively.
- Staff will report, to the Head Teacher, any comments seen on the internet that suggest a child is at risk of a safeguarding issue including radicalisation of any form. Staff will not comment online in response to these types of comments, positively or negatively

Acceptable Use of Technology

(includes e-safety and social media policies)