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 Policy
(A combination Acceptable Use Policy, E-safety Policy and Social Networking Policy.)

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 in promoting the positive uses of technology and the learning benefits it can bring & Trust that they will be responsible in recognising where good choices need to be made.

.

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance and should be read alongside our Child Protection & Safeguarding Policies, it combines e-safety, acceptable use and social networking 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.

The school will provide for each child the relevant KS Digi Safe guide (Appendix 2 & 3) and parental one (Appendix 4) as an easy guide. All concerns should be reported to school's DSL, details are within the school safeguarding policy.

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) to record images, unless permission of the Headteacher has been granted.
- Where images are published (eg on the school website / VLE) 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 Headteacher.
- 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
- 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.

E-safety is taught within our computing curriculum. Our scheme of work fulfils the statutory requirements for computing outlined in the **National curriculum (2014)** and, when used in conjunction with our RSE & PSHE scheme, also covers the government's **Education for a Connected World -2020 edition** framework (see our Education for a Connected World framework mapping).

More information concerning our computing curriculum - https://www.pilgrimscross.co.uk/computing/

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 Headteacher
- No personal information will be shared via email
- Any email received that is deemed to be inappropriate should be reported to the Headteacher 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, unless exceptional circumstances (i.e.family member) and is declared on the Exceptional circumstances for acceptable use of Technology - Appendix 1.
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18, unless an Exceptional circumstance and declared, as above.
- This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- 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 Headteacher 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 Headteacher 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 Headteacher.
- 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 Facebook page and Twitter account are managed by the admin team, 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 least that can be shared the safer the post.
- Any staff blogs run from the school website must be agreed with the Headteacher. The school website should 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 encouraged to have a mobile phone in school
- 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 Headteacher.
- Parents will only be contacted via text using the School texting service, via the school office.
- Staff will not give out their personal mobile phone numbers to children or parents. (Unless due to exceptional circumstances declared on Appendix 1)

S**chool website** :

- The school website is maintained and kept up to date by the Headteacher and the Admin Office.
- The Headteacher 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.
- No content will be uploaded onto the website unless it is agreed by the Headteacher.

C**yber 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 managed by following the school's Anti-bullying Policy.
- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

- All incidents of cyber bullying will be recorded on the schools Behaviour records and parents will be informed. If there is a safeguarding concern then incidents may be refered to other agencies.

Reporting Concerns:

- Any issues relating to staff misuse of the internet must be referred to the Headteacher or Chair of Governors if the concern is the Headteacher.
- Any illegal, inappropriate or harmful material or incident that I become aware of will be report to the Headteacher. In the case where the Headteacher is the alleged perpetrator, I will report to the Chair of Governors.

- **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" on any statement seen on the internet and social media, I will be aware that my 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 or children on the internet, including social media. If I have any concerns then I will share them with the Head teacher or the Chair of Governors.
- Staff will report, to the Head teacher, any negative comments seen on the internet or social media that about any member of staff or the school or are suggesting any type of aggressive behaviour towards any member of the school community. I will not comment online to these types of comments, positively or negatively.
- Staff will report, to the Headteacher, any comments seen on the internet that suggest a child is at risk of a safeguarding issue including radicalisation of any form. I will not comment online to these types of comments, positively or negatively.

INFORMATION FOR PARENTS

Parents will be regularly updated with upto date guidance on how to keep their children safe and how we teach the children how to keep themselves safe online. This information will be shared in the weekly email to parents and more information can be found on our website:

https://www.pilgrimscross.co.uk/computing/
https://www.pilgrimscross.co.uk/internet-safety-1/

Appendix 1
Exceptional circumstances for acceptable use of Technology

Name
Date

I wish the school governors to be aware that the following pupils or ex pupils of the school are 'friends' on my Facebook page/Twitter feed and I have stated the reasons why below:	
These are the minors (children aged between 13- 18) that are 'friends on my Facebook page /Twitter feed: e.g. Billy Smith	Reason for 'friendship' e.g.Nephew