Cranham Church of England (VA) Primary School

E-Safety and Acceptable Use Policy

Authors	Rebecca Slater
Date:	January 2022
Status:	Approved *Subject to addition from KS2 as appendix*
Audience:	Public
Review Date:	January 2024
Teacher Responsible:	Rebecca Slater, Headteacher
Governor Responsible:	Lyn Barker – safeguarding governor

Version	Notes	Date
1	Policy re-write	September 2014
2	Changes regarding: GDPR Relevant technology Safeguarding considerations Acceptable Use agreements for staff and parents added to the appendix.	December 2018
3	No changes	December 2019
4	Policy aims added Relevant terminology Addition of Commerce to complete the 4 C's of online safety.	December 2021

Cranham Church of England Primary School

E-Safety and Acceptable Use Policy

Aims

- To ensure that all pupils are able to use digital devices in school safely, to enhance their learning.
- To ensure that all pupils understand the risks and dangers associated with digital technology (content, contact, conduct and commerce).
- To ensure that pupils know how to reduce these risks both at home and in school.

Context

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Data Protection, Safeguarding and the Staff Code of Conduct.

E-Safety depends on effective practice at a number of levels:

- Responsible use of technology by all staff and pupils; encouraged by education and made explicit through published policies.
- Clear leadership from the lead for Computing on e-safety in the Primary Curriculum
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of web filtering.
- The e-Safety Policy and its implementation will be reviewed every 2 years.
- The policy is approved and monitored by Governors.
- Safe Use of Internet agreements are signed by staff, pupils and parents.

TEACHING & LEARNING

Why use of the Internet is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Enhancing learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This includes both their access on Learn pads and through laptops.
- Pupils will be taught about acceptable Internet use, and given clear objectives for Internet use. Rules will be displayed and there will be targeted lessons on e-safety.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught, through targeted lessons, to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

MANAGING INTERNET ACCESS

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies recommended by Surf Protect will be adopted.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive unsafe/inappropriate e-mail
- Pupils should be taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone (SMART code)
- E-mails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain emails is not permitted.

Published content and the school website

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing images and work

- Photographs that include pupils, carers, staff or visitors will be selected carefully.
- Pupils', carers' or visitors' full names will not be published in digital or traditional media, particularly in association with photographs.
- Written permission from parents or carers and verbal permission from staff, governors and visitors will be obtained before photographs are published in digital or traditional media.
- Pupils' work can only be published with the permission of the pupil and parents.
- Visitors will be advised of the school e-safety policy as appropriate.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of certain social network spaces outside school is inappropriate for primary aged pupils.
- Parents will be informed as and when pupils are involved in blogging activities in school. Only school approved blogging sites will be used.

Managing filtering

- The school will work with an appropriate firewall system to protect pupils and this system is reviewed regularly, and especially after incidents.
- If staff or pupils discover an unsuitable site, it must be reported to the Computing lead. (The monitor will be switched off immediately and a member of staff will later make a note of the undesirable URL. The computing lead will communicate the problem to the firewall provider, so that it may be filtered out.)
- Pupils should be taught to switch off the screen and report any content that concerns them. These incidents are recorded in a log kept by the computing lead.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing

- Pupils should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be a supervised activity.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- The head teacher should be informed in instances where staff require the use of personal mobile phone to teach any session. This should be avoided at all costs.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to General Data Protection Regulations (GDPR).

POLICY DECISIONS

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource (See Appendix 2)
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- All pupil access to the Internet, in both classrooms and in the ICT Suite, will be supervised by an adult.
- Parents will be asked to sign the 'Acceptable use Agreement' (See Appendix 3)
- All staff should be aware of the increased risk of abuse occurring via the internet without the need for the abuser to physically meet the victim.

Pupil mobile phones

- All staff should be aware and make both parents and children aware that if a child brings in a mobile phone into school, it must be left at the office and collected at the end of the day. **They must not be taken into class**. Teachers should not accept / offer children the choice of storing mobile devices in classrooms.
- Any mobiles confiscated from pupils who have failed to hand it into the school office, should be handed in to the school office by the member of staff and a senior member of staff should be made aware.
- All pupils and parents should be informed; children who bring mobile phones into school, do so at their own risk.
- Pupils must not take mobile phones on school trips unless prior agreement has been sought with the head teacher.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school digital device. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher (see Acceptable Use Policy)
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- When suspected criminal or illegal activity has occurred (e.g. by staff or material received/found) the head will refer the matter to the Police and Local Authority.

Community use of the Internet

- The school will liaise with local organisations/ partners to establish a common approach to e-safety.

COMMUNICATIONS POLICY

Introducing the e-safety policy to pupils

- E-safety rules will be displayed and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff should consider all internet use in the light of GDPR and the latest safeguarding guidance.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- There will be an e-safety briefing offered to all parents at least once every two years.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating teacher web directories (Favourites) to demonstrate suitable websites that pupils will be steered towards	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Webquest UK South West Grid for Learning website
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. ∈ Ask Jeeves for kids ∈ Yahooligans ∈ CBBC Search ∈ Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	RM EasyMail SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History See-saw blogging app Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Skype FlashMeeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap Natural History Museum Imperial War Museum

Cranham Church of England Primary School

Staff (and Volunteer) Acceptable Use Policy Agreement

Policy Context

Technologies and the internet, including social media, are powerful tools which provide excellent opportunities for learning and teaching. They can motivate learners, promote creativity, and support effective learning, assessment and engagement with parents. They also bring opportunities to enhance teaching, increase staff efficiency and provide opportunities for staff to benefit from professional development through networking and collaboration. All users have an entitlement to good, safe access to ICT and the internet.

This policy relates to use of all technologies including mobile phones, tablets and online services such as social networking sites. It is intended to ensure that:

- Staff and volunteers are responsible users and stay safe while using technologies
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk from the use of ICT in their everyday work and work to ensure that young people in their care are safe users.
- The organisation is protected from any issues that could negatively affect its reputation

Acceptable Use Policy Agreement

Content

- I know that all school ICT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school.
- I will not upload, download or access any materials which 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.
- I know that internet use is proactively monitored and any illegal activity will automatically result in police involvement
- I will not make large downloads or uploads that might take up internet capacity.

Contact

- I will communicate online in a professional manner and tone and I will not use aggressive or inappropriate language and am aware that any communication could be forwarded to an employer or governors.
- I will only communicate with students / pupils and parents / carers using official school systems.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will only use my own user names and passwords which I will choose carefully so they cannot be guessed easily.

Social Media

- I will only use chat and social networking sites for school purposes that are approved by the school.
- When using social networking sites and other services for personal use I will not say anything that could bring the school, staff members or any member of the school community into disrepute.
- I will ensure that I do not refer to students, pupils, parents/carers or school staff
- I will not engage in any online discussion about the school or any members of the school community unless this is in an approved context e.g. school own Twitter account
- I will not attribute my personal opinions to the school on sites and will make clear that they are my own opinions
- I will immediately report any online discussion that could impact on the school / staff reputation and any negative postings about any member of the school community
- I will not send or respond to friend requests from students on social networking sites.

Conduct

- I will only use school equipment for the purposes of learning and teaching.
- I will not engage in any on-line activity that may compromise my professional responsibilities or compromise the reputation of the school or its members. This includes use of the school e-mail account,

logo or my school role.

- Filtering is provided through the SWGF. I know that, as a staff user, I have access to resources that learners can not access for teaching purposes.
- I will not try and bypass this filtering or access sites that are illegal.
- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement when using it.
- I will not use my personal equipment to record and store images / video of children.
- I will only take images or video of pupils/staff where it relates to agreed learning activities and will ensure I have parent/staff permission before I take them. If these are to be published online or in the media I will ensure that parental / staff permission allows this.
- Where images are published (e.g. on the school website) I will ensure it is not possible to identify the people who are featured by name or other personal information.
- I understand my photograph may be used on the school web site, which means that it could be copied by others. I know that where it is used my photograph will not be accompanied by any personal details.
- I will not install or store programmes on a school device unless I have permission.
- I will not try to alter digital device settings, unless this is allowed in school policies.
- I will not cause damage to ICT equipment in school and will immediately report any damage or faults involving equipment or software.
- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will ensure that I have permission to use the original work of others in my own work and will credit them if I use it. Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Commerce

- I will ensure that I manage financial risks when using school digital devices.

Data Protection

- I understand that our school only uses services which mean that data is stored in line with EU guidelines.
- When I use my teacher laptop at home, I will ensure resources cannot be accessed or copied by anyone else and that no one else uses the laptop.
- I will ensure personal equipment used is password protected.
- I will ensure that my data is regularly backed up.
- I will take all steps within my power to keep personal data safe and minimise the risk of losing it.
- I will only use personal data on secure devices that are password protected.
- When transferring data I will use encryption and secure password protected devices.
- I will ensure that devices I use have approved virus and malware checking software and I will delete data securely once it has been transferred or finished with
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when I am required by law or by school policy to disclose it to an appropriate authority.
- I will not send personal information by e-mail as it is not secure.

Promoting Safe Use by Learners

- I will model safe use of technologies and the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school policy if an issue arises in or out of school that might compromise learner, user or school safety; or if a child reports any concerns.
- I will monitor learner behaviour online when using technology and deal with any issues that arise.

Problems

- I will immediately report any illegal, inappropriate or harmful material; or incident I become aware of, to the e-safety co-ordinator or head teacher.
- If I believe a member of staff is infringing this policy, or putting themselves or others at risk, I will report this to the head teacher.
- **If I believe a young person may be at risk I will follow the child protection procedures.**
- **If I believe a young person may be being bullied via technologies I will follow the anti-bullying procedures.**

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety of other staff and pupils or to the security of the ICT systems.

I understand that these rules are in place to enable me to use ICT safely and that if I do not follow them I may be subject to disciplinary action. I agree to use ICT by these rules when:

- I use school ICT systems at school or at home when I have permission to do so
- I use my own ICT if allowed (including mobile phone or tablet) in school
- I use my own ICT out of school (including mobile phone or tablet) to use school sites or for activities relating to my employment by the school

I know that the school will monitor my use of the school ICT systems and communications.

Problems

- I will immediately report any illegal, inappropriate or harmful material; or incident I become aware of, to the e-safety co-ordinator or head teacher.
- If I believe a member of staff is infringing this policy, or putting themselves or others at risk, I will report this to the head teacher.
- **If I believe a young person may be at risk I will follow the child protection procedures.**
- **If I believe a young person may be being bullied I will follow the anti-bullying procedures.**

Use of Staff Images on School Publicity and Web sites

- I understand my photograph may be used on the school web site, which means that it could be copied by others. I know that where it is used my photograph will not be accompanied by any personal details other than my title and surname.

Staff / Volunteer Name	
Signed	
Date	

Cranham C of E Primary School

Parent / Carer Acceptable Use Policy Agreement

Technologies open up new learning opportunities and can promote creativity, effective learning collaboration and communication. They can promote more effective communications between parents / carers and the school in order to support young people with their learning. **This policy relates to use of all technologies including mobile phones, tablets and online services such as learning platforms and online communications.**

This Acceptable Use Policy is intended to ensure:

- You are aware of what the school is doing to help your child become a responsible user of technology and stay safe at school
- You are aware of the importance of e-safety and are able to support your child with keeping safe and behaving well online at home.

The school will aim to ensure your child has good, safe access to ICT for learning and, in return, expects your child to use the equipment responsibly.

Content

- The school takes every reasonable precaution, including monitoring and filtering systems, to ensure that your child is safe when they use technology at school. The school cannot be held responsible for the nature and content of all materials that are accessible using technology as security systems cannot protect against everything. We teach children about the risks of using technology and how to keep themselves safe.
- We only allow children to use age appropriate web sites in school as using sites for older users can increase the risks to them. This includes social networking sites like Facebook, where the terms and conditions require users to be 13. We appreciate that some parents may allow their children to use sites that they are not old enough for at home. If this is the case then you will need monitor their use and deal with any issues that arise.
- We prevent the use of age inappropriate online gaming sites in school as these can contain adult content and also enable adults to make contact with children online.

Contact

- School policy requires that staff do not make contact with families through social networking sites or personal e-mail addresses but only through agreed school systems. This being the case we hope you will respect this by not requesting to be friends with staff on social networking sites and will understand if staff refuse any friend requests that are made.
- We limit the ability of children to contact each other online in school and use only tools where contact can be limited to others in our school community.

Conduct

- Your child is expected to behave well online as they are expected to during all other school activities.
- Your child will be asked to sign an Acceptable Use Agreement which sets out clear expectations of behaviour when working online. We hope you will talk to your child about this.
- Bullying is not tolerated in any form and this includes online (cyber-bullying). Any instances of this will be dealt with as detailed in our anti-bullying policy.
- Your child will be taught about online safety and how to keep safe when using technology.
- They should only use their own log in for systems and to keep their details private. Your child is responsible for anything their log in is used for.

Commerce

- Your child will be taught about some of the financial risks presented by the internet such as those presented by gambling sites and phishing emails.

Taking Digital Film and Images

- Children and staff may use digital cameras to record learning activities. These images may be used in lessons or to celebrate success through being published in newsletters, on the school website or occasionally in the public media.
- The school will comply with the General Data Protection Regulation (GDPR) and ask your permission, through this policy, before taking images. We will also ensure that when images are published the young people cannot be identified by the use of their names.
- In line with guidance from the Information Commissioner's Office, parents / carers may take videos and digital images of their children at school events for their own personal use as this is not covered by

GDPR. These images must not be published or made available on social networking site in order to protect other children and respect privacy. Parents / carers should also not comment on any activities involving other pupils in the digital / video images.

Problems

- We can only take responsibility for e-safety issues that happen in school, or at home when children are using sites recommended by the school.
- Any issues you are made aware of with use of technology in school should be reported immediately to a child's teacher so that appropriate steps can be taken.
- If your child does not behave appropriately online then the school will take steps to deal with this as with any other issue with behaviour.
- You are obviously responsible for your child's safety online when at home and we would hope you will be discussing e-safety with your child and monitoring their use of computers and mobile phones.
- If there is an issue occurring outside school that it may be helpful for us to be aware then please let your child's teacher know. While we do not have responsibility to resolve all issues we may be able to deal more effectively with any implications happening in school and adapt our teaching programme to ensure that these issues are covered.

Permission Form

We request that you sign the permission form below to show your support of the school in helping to keep your child safe. By signing this form you are agreeing that:

- Your child can use school technology and online services for learning
- You have read and discussed the rules with your child
- You understand the rules that your child should be following when using ICT in school and this also applies to their use of their mobile phone
- You give permission for taking and using images of your child for learning purposes

Parent / Carers Name		Date	
Student / Pupil Name			

Home Use of the Internet

We hope you will reinforce the e-safety messages when your child uses the internet at home. Some ways that you could do this are listed here to support those of you who may not be aware of all the issues. With the large number of mobile devices it is now very difficult to supervise all access to the internet, however you will want to set age appropriate rules for using technology at home. The school rules could be a starting point.

Content

- Make sure content is appropriately filtered for younger users.
- Make sure your child knows that a protection system does not stop all unsafe content and they need to tell you if they access something inappropriate or get an upsetting message.

Contact

- Talk about the need to be polite online and that they should not use bad language or comments which might upset others.
- Discuss the fact that e-mails / messages can be intercepted and forwarded on to anyone (including parents, head teacher or future employer!).
- Make sure they know they should not open messages if the subject field is offensive or if they do not recognise who it is from and that the safest thing to do is to delete it without opening it.
- Ensure that any online games they are using are of an appropriate age rating and make sure they are aware that they could be contacted through games and not to give out personal information.

Conduct

- Talk to your child about the fact that any information published on the web can be read by anyone and that they should only post things they would be happy for anyone to read.
- Check that they are old enough for the sites they are using. If you allow them to use a site they are not old enough for ensure that you have access to what they are doing so that you can monitor it.
- Make sure that family digital devices are password protected and have anti-virus software which is regularly updated.
- Ensure that your child knows not to leave digital devices logged on with their user name or logged on to sites with personal details entered as others could use them.
- Discuss user names and talk about how to choose them carefully to protect their identity.
- Talk about the information children should keep private in order to stop them being contacted including full name, direct e-mail, address, telephone number, school and places they go regularly. Check information that younger users are publishing to ensure that they are not putting themselves at risk. This includes any personal information which could lead to someone being able to contact them.
- Ask your child about the sites they are visiting.
- Talk about using the safety and privacy features of sites to only give access to people they know and to be careful who they add as friends.
- Make sure they know that downloading copyrighted games and music without paying for it is illegal.
- Remind them they should not respond to offers they have not requested as these could be scams, result in costs or be trying to find out their personal information.
- Remind them that they should not purchase or download anything that costs money without asking permission and that they should not use someone else's identity to buy things online.

Problems

- Make sure they know that if they get any problems with using digital devices or get an offensive or worrying message / e-mail they should not reply but should save it and tell you.
- Please tell the school of any concerns that you have or anything that they could help to address through teaching.

Reassure your child that if they talk to you about a problem online you will not ban them from going online as this will discourage them from telling you.