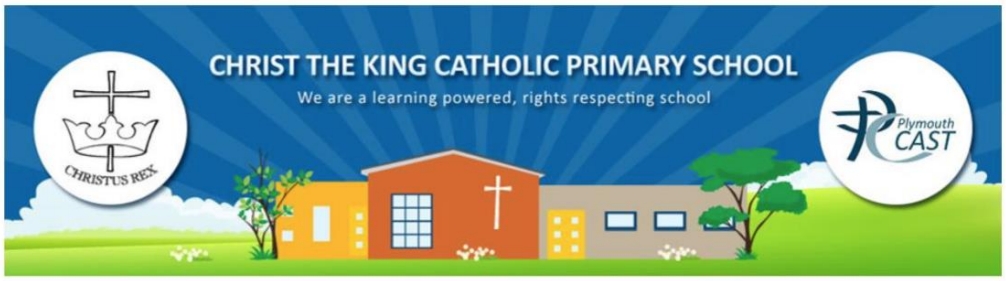


ONLINE SAFETY POLICY

Introduction to Online Safety Policy

Our online safety policy will operate in conjunction with other policies including those for pupil behaviour, anti-bullying, curriculum, data protection and security. It involves all members of staff from the Headteacher to any new member of staff. Through its compliance it will ensure that everyone knows and understands their responsibilities and can act upon them.

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy is specific to Christ the King RC Primary School and adheres to the guidelines set by SWGfL regarding online safety.

Who are SWGfL?

The South West Grid for Learning Trust is an educational trust that has an international reputation in supporting schools with online safety. SWGfL, along with partners Childnet and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. SWGfL is a founding member of UKCCIS (UK Council for Child Internet Safety) and has spoken at conferences across Europe, America and Africa. More information about its wide ranging e-safety services for schools can be found on the SWGfL website – www.swgfl.org.uk.

This e-safety policy was approved by the LGB on February 2022

The implementation of this online policy will be monitored by: e-Safety Champion and the Senior Leadership Team.

Due Date for next review: February 2024

Availability of the policy: The policy can be viewed on the school website www.ctkcps.com . A paper copy is displayed on the Safeguarding Notice Board in the School Staffroom.

Should serious online safety incidents take place, the following external persons/ agencies should be informed: SSCT (Safer School Community Team) See also Appendix A.

The school will monitor the impact of the Policy using:

- **Reported incidents on CPOMS.**
- **Surveys/ Questionnaires of pupils and staff.**
- **Audits will be carried out by the e-Safety Champion and the Senior Leadership Team.**

S

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Improve Learning?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data within Plymouth CAST;
- access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable Information Use Agreement' (Appendix C) before using any school ICT resource, including trainee teachers.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to return a form if they wish to deny pupil access on-entry to Foundation Stage. A copy is available from the school office.

World Wide Web

- **If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the e-Safety Champion, IT Subject Leader and IT Technician.**
- **School will ensure that the use of internet derived materials by staff complies with copyright law.**
- **Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.**

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils are taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Only whole class, group or school allocated e-mail addresses may be used in school.
- E-mailing and receiving from external email accounts is blocked for pupil addresses.
- Access in school to external personal e-mail accounts is blocked.
- The forwarding of chain letters is not permitted.

Social Networking (see separate guidelines for Social Networking use)

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils are told not to access any social network space.
- Pupils are advised on security and encouraged to set strong passwords, deny access to unknown individuals and how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.

Filtering

The school sets up their own filtering and will work to ensure filtering systems are as effective as possible.

Managing Emerging Technologies

- Emerging technologies are examined for educational benefit and a risk assessment carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Website

- The contact details on the website are the school address, e-mail and telephone number. staff or pupils personal information will not be published.
- The Head Teacher and ICT Technician will take overall editorial responsibility and ensure that content is accurate and appropriate.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images. However the school reserves the right to not allow photography or recording of particular school events.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Parents and carers will be requested to give their permission for their child's image to be used on the school website as part of their enrolment and annually thereafter.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection Principles

The GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Refer to the Trust Data Protection Policy for further information.

Information System Security

- School ICT systems capacity and security are reviewed regularly.
- Virus protection is installed and updated regularly.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Plymouth CAST can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

Handling online safety Complaints

- A senior member of staff will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

A copy of the Trust's complaints policy is available on the school website.

Communication of Policy

Pupils

- Pupils are informed that Internet use is monitored.
- Each pupil in school receives an update and refresher of Online Safety training as part of their computing lessons at least once every half term. This equates to a minimum of 6 hours per academic year. See Appendix B. The aim of the update is to ensure that each pupil has a good understanding of research skills (avoiding plagiarism and upholding copyright regulations), understands the importance of reporting abuse and misuse, and adopts good online safety practice when using digital technologies both inside and outside of school.

Staff

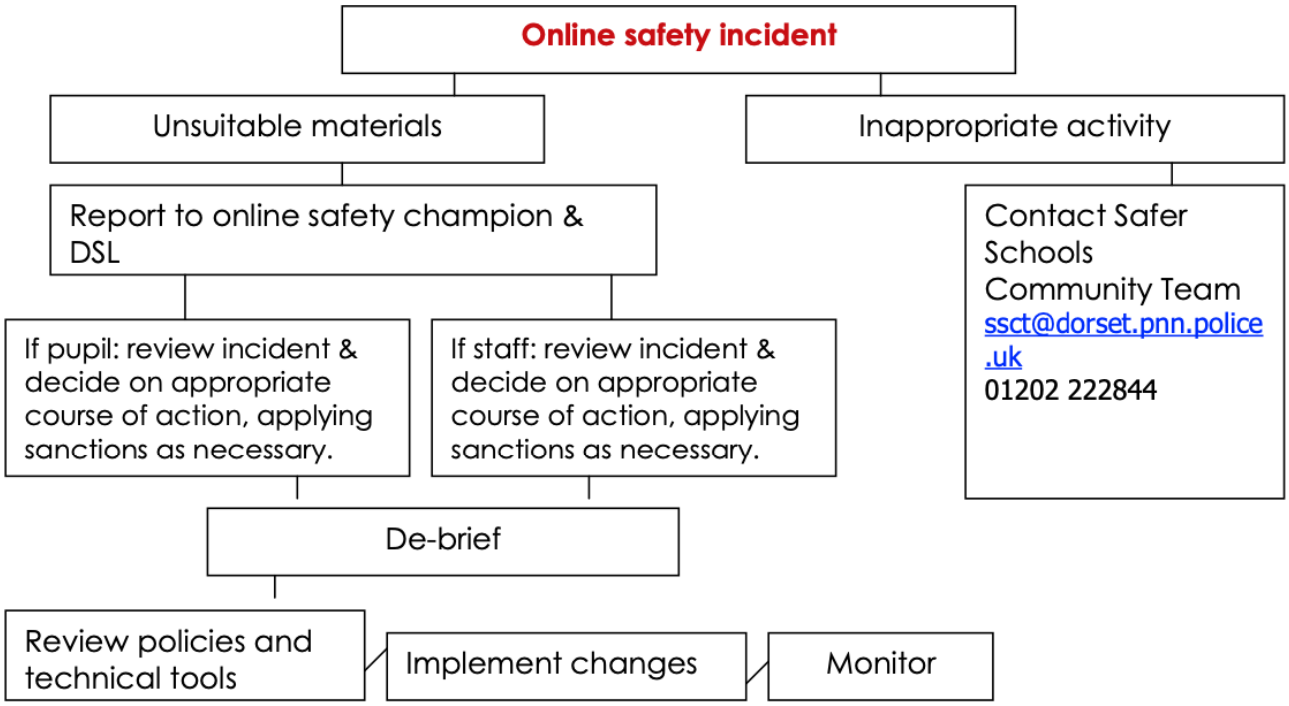
- All staff are given access to the School Online Safety Policy as part of their induction when they join the school. A paper copy of the Policy is displayed on the Health and Safety Notice board in the staff room.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. See Appendix B.

Parents

- Parents and carers play a crucial role in ensuring that their children understand the need to use both the internet and mobile devices in an appropriate way. The school will take every opportunity to make them aware of the School Online Safety Policy via newsletters, the school Prospectus and the school website.

Referral Process – Appendix A

Flowchart for responding to online safety incidents in school.



Adapted from BECTA - Online safety 2005

Online safety Rules – Appendix B

Online safety Rules

These online safety rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or an illegal purpose is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

Key Stage 2

Think then Click

These rules help us to stay safe on the Internet

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any web page we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Staff Acceptable Information Use Policy – Appendix C

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's online safety policy for further information:

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data (in paper or electronic format) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Sensitive electronic data will be encrypted if taken off site.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school online safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

Staff have been made aware that breaches of this code of conduct that, for example, result in a child's personal details coming into the public domain, may be investigated by the Information Commissioner and may result in a substantial fine of up to five million pounds.
The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

	Staff and other adults			Pupils	
Communication Technologies	**Not allowed**	**Allowed out of teaching time**	**Allowed at certain times**	**Not Allowed**	**Allowed with staff permission**
Mobile phones may be brought to school		✓		✓*	
Use of mobile phones in lessons	✓			✓	
Use of mobile phones		✓		✓	
Taking photos on personal mobile phones / cameras	✓			✓	
Use of other mobile devices eg tablets, gaming devices		✓+			✓
Use of personal email addresses in school, or on school network		✓		✓	
Use of school email for personal emails	✓			✓	
Use of messaging apps			✓		✓
Use of social media			✓		✓
Use of blogs			✓		✓

***Must be handed in to the office**
+in office / staffroom spaces only

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …….. Print Name: …….. Date: ……