



St Anne's C of E (A) Primary School E Safety and Acceptable Use Policy

'Let all that you do be done in Love' 1 Corinthians 16:14

St Anne's strives to *'develop the whole child, spiritually, mentally and physically by helping pupils to:*

Love God

Love learning and

Love themselves and others

in a caring, Christian environment through close links to the Church and community.

Approved by	Approval date	Review date
FGB	October 2015	Autumn 2019
FGB	06.11.2019	Autumn 2022

Writing and reviewing the e-safety policy

Our e-Safety Policy has been written by the school, following government guidance. It relates to other policies including those for ICT, Anti – bullying and safeguarding children.

- It has been agreed by senior leadership and approved by governors.
- The e-Safety Policy and its implementation will be reviewed.
- It is available to read or download on our website or as a hard copy from the school office.

Roles and Responsibilities

The school has an e- safety team in conjunction with the Safeguarding team and ICT.

Teaching and learning

Why Internet and digital communications are important

- The purpose of technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- 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.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to the wider audience.
- They will be taught how to report unpleasant content including Cyberbullying or unwanted contact.
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self – efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the LA as required.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- All incoming email should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school web site

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

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
Pupils' full names will not be used anywhere on the website or Blog, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site; it may need monitoring and educating the students in their use.
- 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 social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable in partnership with the ICT bought in support.
- Should staff or pupils discover a way to circumnavigate filtering this will be reported to the E-safety coordinator.

Managing video conferencing

- Videoconferencing will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving a video conference call.
- Videoconferencing will use the educational broadband network to ensure quality of service and security.

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 and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required. The coordinator will monitor access to school network.
- Staff will be issued with a school phone where contact with pupils and their families is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and protected in accordance with Data Protection Act 1998. Authorised individuals will oversee this.

Policy Decisions

Authorising Internet access

- All staff must read the 'staff code of conduct', set out in Appendix 2 before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted access to school IT systems. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific approved on-line materials.
- Any person not directly employed by the school will be asked to sign an 'Acceptable Use of School ICT resources' before being allowed to access the internet from the school site.

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 computer.
- Neither the school nor LA 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 headteacher.
- 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 consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

Community use of the Internet

All use of the school internet connection by community and other organisations shall be in accordance with this e-safety policy, and such users will be required to sign an acknowledgement to say that they have read and understood this. (see Appendix 2)

Communicating the Policy

- E-safety rules will be posted in all class rooms and ICT areas and discussed with the pupils at the start of each year.
- Appropriate elements of the e-safety policy will be shared with pupils.
- Pupils will be informed that network and Internet use will be monitored.

Appendix 1

E - Safety Agreements and Rules

E Safety Rules for Key stage 1

E safety rules for Key Stage 2

Think Before You Click

These rules help us to stay safe on the Internet

- I only use the Internet when an adult is with me.
- I can click on the buttons or links when I know what to do.
- I can search within websites chosen by an adult.
- I always ask if I get lost on the Internet.
- I can send and open emails together.
- I can write polite and friendly emails to people I know.

Think Before You Click

These rules help us to stay safe on the Internet

- I only use the Internet if I have permission
- I can search within websites chosen by an adult.
- I will tell an adult if I see anything I am uncomfortable with.
- I will only email people an adult has approved.
- I will send and post messages and comments that are polite and friendly.
- I will never give out passwords or personal information.
- I will not open emails sent by anyone I don't know.
- I will not use internet chat rooms.
- I will never arrange to meet anyone new that I have only chatted with on line.

Staff, Governor and Visitor Acceptable Use Policy/ICT Code of Conduct

ICT and the related technologies such as emails, the internet and mobile devices are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its content.

- I appreciate that ICT includes a wide range of systems and devices including mobile phones, digital cameras, email, social networking and may include some personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or any other related authorities.
- I understand that I am responsible for all activities carried out under my username.
- I will only use the school email, internet, intranet or any related technologies for professional purposes.
- I will ensure the personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the head teacher or governing body.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with the consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without permission.
- I will ensure that my online activity both in and outside of school will not bring my professional role, school or colleagues either explicitly or by implication into disrepute.
- I will ensure that all electronic communications with parents, pupils and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's e-safety policy and help pupils to be safe.
- I will report any incidents of concern regarding children's safety to the e-safety coordinator, the head teacher or safeguarding team.
- I understand that sanctions for disregarding the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

I agree to follow the code of conduct and support the safe use of ICT throughout the school.