ST ANNE'S
FULSHAW

Over 125 years of achievement

Online Safety Policy

St Anne's Fulshaw CE Primary School Online Safety Policy

Online safety: The Rationale

Online safety encompasses the use of all technologies and electronic communications. 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 on line experience.

The school's Online Safety Policy will operate in conjunction with other policies including those for behaviour, anti-bullying, data protection and acceptable use

Objectives of the Policy

The objectives of this policy are to ensure:

- our children and staff are protected as far as reasonably possible when using the internet and other online tools
- responsible IT use by all staff and students, encouraged by education
- secure school network design and use
- a safe and secure broadband from an approved Internet Service Provider using suitable filtering
- the safe use of the internet by children and staff

What does electronic communication include?

- Internet collaboration tools: social networking sites and blogs
- Internet Research: web sites, search engines and Web browsers
- Mobile Phones, personal digital assistants (PDAs), and any other hardware that allows internet access such as iPods/iPads
- Internet communications: email and instant / direct messaging / WhatsApp
- Webcams and videoconferencing

What are the risks?

Receiving inappropriate content	Publishing inappropriate content
Predation and grooming	Online gambling
Requests for personal information	Misuse of computer systems
Viewing 'incitement' sites	Publishing personal information / images
Bullying and threats	Hacking and security breaches
Identity theft	

Strategies to promote online safety:

- All staff will continue to promote online safety to pupils through the curriculum and PSHE offer
- Online safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and internet use will be monitored.
- Pupils will be taught why the internet is important and how it can be used to enhance learning - the internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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's internet access will be designed expressly for pupil and family 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.
- 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 to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Internet access through the school will be appropriately managed
- School IT systems and security will be reviewed regularly.
- Virus protection will be installed on every computer and will be set to update automatically when necessary.
- Pupils will be taught to use email appropriately
- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must be taught not to reveal personal details (ie full name, address, school) of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- When using class Twitter feeds, only first names will be used
- Email sent to an 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 letters or other inappropriate email is not permitted.
- The school will monitor any published content and the school web site
- The contact details on the web site should be the school address, e-mail and telephone number.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Publishing of pupil's images and work should be carefully considered and only undertaken in line with the parental permissions given at the start of a pupil's time in the school
- The Headteacher routinely monitors images published on the school website, Twitter accounts and local press
- Pupils' full names will not be used in association with photographs, except where parents have given direct permission for them to appear in the local newspaper.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.
- Pupils will be taught safe practice in using social networking sites and personal publishing
- The school will filter and monitor access to social networking sites.
- When managing their online presence pupils will be advised never to give out personal details of any kind which may fully identify them or their location (ie full name, full address, school).
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Staff are advised that they should consider the consequences and possible repercussions of any information that they make available online, for example on a social networking site. The posting of photographs, videos and

information related to the school, school life, other staff and pupils on personal accounts is not permitted.
- The Headteacher will ensure systems to manage the filtering of websites is kept up to date
- The school will work with the LA, DfE 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 Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will maintain systems for the safe management of video conferencing
- Pupils must ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the pupils' age.
- Emerging technologies will be reviewed for potential risk and use in schools
- 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.
- Staff will not use personal equipment or non-school personal electronic accounts when contacting students
- The school will protect personal data
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- Authorisation is required before internet access is allowed
- All staff must read and sign the 'Safeguarding Code of Conduct' before using any school IT resources.
- The school will keep a central record of all staff and pupils who are granted network access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Within the school access to the internet will be supervised.

Handling online 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 and referred to the DSL or Deputy DSL.
- Pupils and parents are informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues

Staff and the online safety policy

All staff will be given the school Online 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 and expected.

Enlisting parents' support

Parents’ attention will be drawn to the school Online Safety Policy in newsletters, the school brochure and on the school web site. Parents will be given opportunity to attend internet safety awareness events and training when available.

Role of the IT Subject Leader

The subject leader will monitor the implementation of the Online Safety Policy throughout the school. They are responsible for promoting the continued good practice of highlighting online safety. They are responsible for keeping themselves and the staff up to date with relevant developments in IT and any changes to the policy that arises. They are responsible for monitoring curriculum provision, schemes of work and teaching and learning to ensure that all aspects of the IT curriculum including the teaching of online safety, and report to the Headteacher and / or Governors, any issues that develop in relation to online safety and in particular could impact upon the safety of staff or children. They have a significant role in ensuring systems are in place to enhance the school’s child protection and safeguarding procedures.

The school will take all reasonable precautions and measures to ensure that users access only appropriate material. However, due to the 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 the local authority can accept liability for the material accessed, or any consequences of internet access.

The Online Safety Policy and its implementation will be reviewed annually to reflect the rapid changes in technology.

The school will regularly audit IT provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

Reviewed 10.10.22