



Living Life in all its Fullness - John 10:10

KIRK FENTON CE PRIMARY SCHOOL

E-Safety Policy

January 2020

Review Date: Spring 2023

Our Vision

Rooted in Christian belief, our vision for every member of this school community is to feel valued and respected, regardless of age, gender, sexuality, race, faith, belief or ability. Through developing a love of learning, each individual will have the opportunity to reach their full potential and aspire to become the person they were born to be.

Let your light shine before others, that they may see your good deeds and glorify your Father in Heaven. Matthew 5:14-16

Rationale

E-Safety encompasses Internet technologies and electronic communication such as mobile phones and wireless technology. In society in general, children are regularly exposed to social media, gaming and advertising on many different types of device. E-Safety highlights the need to educate children and young people about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to own and control their online experiences.

The E-Safety Policy at Kirk Fenton CE Primary School operates in conjunction with other policies including the Behaviour Policy, Anti-Bullying Policy, Child Protection and Safeguarding Policy, Curriculum Policy and Data Protection Policy. All of these can be found on our school website or are available from the school office.

Scope of the policy

This policy applies to all pupils, staff and governors of the school as well as any visitors to the school.

Good Habits

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

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through lessons and published policies.
- Sound implementation of the E-Safety policy both in administration and curriculum, including a secure school network design and usage.
- Safe and secure broadband from the provider including the effective management of content filtering (through NYCC)
- National Education Network standards and specifications
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF (Internet Watch Foundation) or CEOP (Child Exploitation & Online Protection Centre).

Dangers to Consider

Some of the dangers children may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/ loss of/ sharing of personal information
- The risk of being subject to grooming by those whom children contact on the internet
- The sharing/ distribution of personal images without an individual's knowledge or permission
- Inappropriate communication or contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video or internet gaming

- An inability to evaluate the quality, accuracy or relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Excessive usage impacting on social and emotional development

As with all things, it may be impossible to eliminate all risk completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has done everything that could reasonably be expected of it to manage and reduce these risks. This E-Safety Policy explains how we intend to do this.

School E-Safety Policy

The school E-Safety Coordinator is the Designated Safeguarding Lead, currently Mrs Williams.

Our E-Safety Policy has been written by the school, building on Government and the Star Multi-Academy Trust policy. It has been approved by the school governors.

The policy will next be reviewed in Spring 2023.

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.

Many 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 Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums, art galleries and online learning platforms;
- 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 with the Local Authority and DCSF;
- access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised internet access whilst in school.
- Parents and pupils are asked to sign the school's Home/School Agreement which includes guidelines for internet usage.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk and the Star Multi-Academy Trust via the e-safety coordinator or other senior member of staff.
- Teachers will ensure that the use of internet derived materials 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 and Online Collaboration (Google)

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail or messages.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised by a teacher before sending, in the same way as a letter written on school headed paper.

- The forwarding of chain letters is not permitted.

Social Networking

- The School blocks/filters access to social networking sites and newsgroups 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 should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority, The Star Multi-Academy Trust and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Videoconferencing will be appropriately supervised for the pupils' age and take place as a whole class through a staff account.

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.
- Pupils are not allowed to bring mobile phones into school unless prior permission has been granted. Where this is the case, pupil mobile phones should be handed into the school office upon arrival at school and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Web Site

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

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

- Pupils' names will not be used anywhere on the Web site or social media in association with photographs.
- Written permission is obtained from parents or carers before photographs of children are published on the school website or social media.
- Pupils' work will only be published with the permission of the pupil and will not be named.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and updated regularly.
- Security strategies will be discussed with the The Star Multi-Academy Trust and broadband provider.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and current GDPR Regulation.

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, the STAR MAT nor NYCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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.
- Parents wishing to complain about e-safety issues should use the established school complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all classrooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- Staff will be given a copy of the E-Safety Policy regularly and a copy will be included with the Induction Policy for new staff
- All staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Website.