St. Andrew's CE (VA) Infant School and St. Andrew's CE (VA) Junior School

E-Safety Policy

Title	E-Safety Policy
Version	1.1
Date	September 2019
Author	Mrs Nicola Martin
Approved by headteacher	December 2018
Approved by governing body	
Next review date	December 2022

Modification history			
Version	Date	Description	Revision author
1.1	02/10/19	Information added from Policy Review February 2019	Stephanie Hardaker (Administrator)

E-Safety Policy

Rationale

We are committed to safeguarding and caring appropriately for every aspect of the lives of the children at both St Andrew's Infant School and St Andrew's Junior School. Together, we recognise our responsibility to take action on behalf of all children and others who are, or may be, at risk of neglect from physical, sexual or emotional abuse at the hands of any other person. The statutory curriculum expects pupils to learn how to locate, explore and exchange information using ICT. In delivering the curriculum, teachers need to plan for and make use of communications technology. Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop ICT life skills to support this. The primary concern for teachers, with regard to the online environment, is the safe and effective supervision of pupils using the internet and educating pupils on what to do to avoid risk and report any internet abuse, by highlighting some of the associated risks and ways to deal with them, if encountered. We must not only protect pupils when they are in our care, we must also educate them to apply their understanding for when they work outside the school environment.

School Responsibilities

This policy has been developed in conjunction with the Calderdale Internet and E-mail Usage Policy and will be approved by Governors and reviewed annually. Each school has their own person responsible for E-Safety, this is the Designated Person for Child Protection (DPCP).

Teaching and Learning

Internet use is part of the statutory curriculum, a necessary tool for learning and an essential element in 21st century life for education, business and social interaction. At St Andrew's, children use the internet on a daily basis. The school has a duty to provide children with quality and safe Internet access as part of their learning experience via specific sites or using Google. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care for their own safety.

<u>Internet Benefits in Education:</u>

- 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
- 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 DfE
- Access to learning wherever and whenever convenient

To enhance learning: Pupils will be

- Taught what Internet use is acceptable and what is not, and be given clear objectives for Internet use.
- Educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Staff should guide pupils in on-line activities to support learning outcomes planned for the pupils' age and maturity.

How will pupils learn to evaluate Internet content?

As our pupils move into KS2 they will begin to use the Internet more widely outside school. We will encourage the children to evaluate on-line materials and to take care of their own safety and security, being aware of the CEOP report abuse button.

Managing Information Systems - Security of the school information systems

• The security of the school information systems will be reviewed annually by the IT Coordinator. Virus protection will be updated regularly by Pure Technology/Calderdale IT and security strategies will be discussed with them.
• Personal data sent over the Internet will be encrypted or otherwise secured.
• Portable media must not be used without first undergoing a virus scan.
• Pure Technology/Calderdale IT manage our IT system and will review system capacity regularly.

Managing e-mail

Pupils will not have access to a school email account. Staff emails sent to external organisations on behalf of the school should be written carefully. The forwarding of chain letters is not permitted using school email addresses. Staff should NEVER send personal data via email unless the email is securely encrypted.

Home Working

Personal data should not be accessed on a home computer, laptop or tablet unless staff have up-to-date anti-virus/anti-malware.

Managing Published Content

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright. E-mail addresses should be published carefully, to avoid spam harvesting.

Publishing pupil images and/or work

Images that include pupils will be selected carefully to use on the school website/school

Facebook page. A letter will be sent out when a child starts school assuming that this can take place unless a parent writes stating that they wish their child to be excluded from this.

Social networking and personal publishing
The YHGfL blocks access to all social networking sites in school.

Filtering
• The school's Internet filter will be provided by the LA in conjunction with YHGFL.
• If staff or pupils discover unsuitable sites, the URL must be reported to the IT Coordinator.
• Any material that the school believes is illegal must be reported to appropriate agencies such as YHGFL or CEOP by the Head Teacher.

Emerging Technologies
• New technologies will be examined for educational benefit and a risk assessment will be carried out before such technologies are used in school.
• Children will not be allowed to have a mobile phone in their possession in school. If one is accidentally brought to school, it must be switched off and handed in to the adult in charge of the class, who will store it until home time.
• The school will investigate wireless communication technologies.

Personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
Any ICT software that requires personal information will be subject to a Data Protection Impact Assessment by the Data Protection Officer before use. The school will only use ICT software providers that are compliant with Data Protection laws.

Authorising Internet access
• At the start of Reception, parents will be informed that pupils will be provided with supervised Internet access throughout their schooling at both St Andrew's Schools and will be asked to inform the Head Teacher in writing if they do not wish their child to access the internet at school.

Risk Assessment
The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor YHGFL can accept liability for the material accessed, or any consequences resulting from Internet use.

E-Safety Complaints

Complaints about staff or children's Internet misuse will be referred to the Head Teacher/Designated Person for Child Protection and the School's Complaints Procedure will be followed. All incidents will be recorded. All involved will be carefully questioned by the DPCP to understand the case, working in conjunction with the Local Authority Designated Officer (LADO) – ***Children's Social Care, Lower Valley Team: 01422 373491*** in extreme cases and reporting incidents to CEOP (Child Exploitation Online Protection) via the CEOP website: *www.ceop.police.uk*

Introducing the Policy to Pupils

Basic e-safety children's training will be introduced to raise the awareness and importance of safe and responsible internet use throughout the year in every year group to ensure children know what to do to keep safe when using the internet. Instruction in responsible and safe use should precede Internet access. Rules for using the internet will be posted near computers and explained to the children.

Parents' Support

Parents' attention will be drawn to the school's e-safety policy. Internet issues will be handled sensitively, and parents will be advised accordingly.

Consultation, Monitoring and Review

This policy will be reviewed annually to ensure adequacy and appropriateness. Any changes made based on the review will be documented and all staff informed.

Policy Review:

This policy should be reviewed within 12 months of the date it was written.