E Safety Policy
2021-22

Approved by:	Headteacher	**Date:**	October 2021
Last reviewed on:	15th October 2021		
Next review due by:	October 2022		

In light of our mission statement and our anti-discrimination policy, the staff and governors of St Ambrose RC Primary School have set down the following policy for E-Safety.

Aim

The aims of this policy are to establish clear guidelines for E-Safety in our school to ensure equality of opportunity for pupils.

This policy is to be read in conjunction with our Safeguarding, Behaviour, Computing, Anti-Bullying, RHE and Staff Code of Conduct policies, Also, this policy takes guidance from 'Keeping Children Safe in Education' 2021 (KCSIE).

St. Ambrose RC Primary school follow the MSP guidelines 'Safeguarding online guidelines for minimum standards' and the advice on the UK Safer Internet Website.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk (KCSIE):

• **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

• **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel our pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group.

Teaching and Learning

The Internet is an essential element in life for education, business and social interaction. We have 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 internet will enhance learning. School internet access is designed expressly for pupils use and uses 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.

The National Curriculum states that pupils should be taught to:

Digital Literacy	**Key Stage 1** Recognise common uses of information technology beyond school. Use technology safely and respectfully, keeping personal information private;	**Key Stage 2** Understand the opportunities networks offer for communication and collaboration. Be discerning in evaluating digital content.

	identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.	Use technology safely, respectfully and responsibly; Recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

The children are taught to 'Be SMART Online'

SAFE Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

MEETING Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk

ACCEPTING Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

RELIABLE You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

TELL Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk

Digital Leaders

Digital Leaders are children who want to share their knowledge with others and promote the use of all things digital throughout the school. Being a Digital Leader is a fantastic opportunity for children and it enables them to take on responsibility, learn new skills, develop and demonstrate leadership skills and be a real help to staff and children. Digital leaders will help share with children how to stay safe online and lead assemblies that promote being 'SMART' online.

Staff Training

All staff access training for Online safety through annual safeguarding training. Online safety modules are completed at least every other year on Educare. Online safety and the teaching of digital literacy is planned for during half-termly planning meetings. Training is part of the induction process for new members of staff.

World Wide Web

If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the ICT support helpdesk by the relevant member of staff or class teacher.

School will ensure that the use of Internet derived materials by pupils and 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.

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. The school cannot accept liability for the material accessed, or any consequences of internet access.

Email

Whole class or school e-mail addresses should be used when communicating with children. These will only be used during periods of remote education.

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-mails sent to external organisations by staff should be written carefully and in the same way as a letter written on school headed paper.

Social Networking

School has blocked and filtered access to social networking sites and newsgroups except when a specific use is approved for staff. The school works with One Education ICT Support to ensure filtering systems and firewalls are effective as possible.

Pupils are taught never to give out personal details of any kind which may identify them or their location.

Pupils are taught not to place personal photos on any social network space.

Pupils are taught about security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are taught and encouraged to invite known friends only and deny access to others.

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.

In line with the Staff Code of Conduct, mobile phones will not be used for personal use during school hours. The sending of abusive or inappropriate text messages is forbidden. Children are not allowed to bring mobile phones into school. If they are brought in they are kept in a locked drawer in the office.

Published Content and the School Website

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 headteacher and senior leadership team will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Work and photographs

Parental consent is sought at the start of every school year or on admission prior to publication. Pupils' full names and other personal information are be omitted. Separate consent is sought for photos on the school website, social media sites and use on third party websites and social media.

Information System Security

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

Protecting Personal Data Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Role of Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- Google Classroom

Advice for Parents

Don't wait for something to happen before you act. Make sure your child understands how to use these technologies safely and knows about the risks and consequences of misusing them.

Make sure they know what to do if they or someone they know are being cyber bullied. Encourage your child to talk to you if they have any problems with cyber bullying. If they do have a problem, contact the school, the mobile network or the Internet Service Provider (ISP) to do something about it.

Parental control software can limit who your child sends emails to and who he or she receives them from. It can also block access to some chat rooms. Moderated chat rooms are supervised by trained adults. Your ISP will tell you whether they provide moderated chat services.

Make it your business to know what your child is doing online and who your child's online friends are. It is important that parents and carers ensure that their children are engaged in safe and responsible online behaviour.

Suggestions for parents to stay involved

Keep the computer or other electronic devices in a public place in the house. Periodically check on what your child is doing.

Discuss the kinds of internet activities your child enjoys.

Be up front with your child that you will periodically investigate the files on the computer, the browser history files, and your child's public online activities.

Search for your child's name online, look at his or her profiles and postings on community sites, social media sites or blogs.

Tell your child that you may review his or her private communication activities if you have reason to believe you will find unsafe or irresponsible behaviour.

Watch out for secretive behaviour as you approach your child when they are online, such as rapidly switching screens, changing passwords and for attempts to hide online behaviour, such as an empty history file.

Incidents of Online Technologies Misuse

Incidents of misuse will be dealt with in accordance with our safeguarding reporting procedures and reporting of bullying incident. Incidents of staff misuse of technology will be brought to the attention of the headteacher and will be dealt with directly by the headteacher.