St Andrew's
Primary School
growing together

ONLINE SAFETY POLICY

Reviewed: October 2023

ST ANDREW’S C of E PRIMARY SCHOOL

ONLINE SAFETY POLICY

RATIONALE

St Andrew's School is a place where everyone is valued and cared about. Our vision and ethos is growing together to unlock potential through a curriculum where pupils thrive and develop character and master knowledge and skills within a Christian community where everyone is valued and cared about. We believe in growth mindsets and that all children can learn without limits. This means that we don’t set a ceiling or a limit on what any individual is able to do. We trust our children with support to make their own decisions and to challenge themselves and grapple with their own learning.

GUIDELINES

This policy sets out the ways in which the school will:

- Educate all members of the school community on their rights and responsibilities with the use of technology
- Build both an infrastructure and culture of Online Safety
- Work to empower the school community to use the Internet as an essential tool for lifelong learning.

The impact of the policy will be monitored by the Online Safety Lead by looking at:

- Log of reported incidents
- Surveys or questionnaires of learners, staff, parents and carers
- Other documents and resources

ROLES AND RESPONSIBILITIES

The Headteacher is responsible for ensuring the safety (including online safety) of all members of the school community, though the day to day responsibility for online safety can be delegated.

An Online Safety Leader will be appointed, (Mrs N Gee) who, working with the Designated Safeguarding Lead and Deputy Safeguarding Lead, will have overview of the serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

Online safety will be discussed during children's treehouse groups three times a year and followed up by teachers with their classes. Online safety is delivered alongside our computing curriculum and we have annual online safety workshops in school which are delivered by a Cyber Protect Officer. Staff also receive training in online safety.

Role	Responsibilities
Governors	Approve and review the effectiveness of the online safety policy Delegate a governor to act as online safety link

Head Teacher and Senior Leaders	Ensure that all staff receive suitable CPD to carry out their online safety roles Create a culture where staff and learners feel able to report incidents Follow correct procedure in the event of a serious online safety allegation being made against a member of staff or pupil Inform the local authority about any serious online safety issues Ensure that the school infrastructure/network is as safe and secure as possible
Online Safety Leader	Plan for online safety to be discussed at treehouse groups three times a year Keep parents/carers informed about online safety via the school newsletter and social media. Set up and run a working online safety group with pupils Work with IT support to ensure strict filtering and monitoring processes are in place Review online safety policy and practice regularly using 360 safe Lead the establishment and review of online safety policies and documents Ensure all staff are aware of the procedures outlined relating to online safety Meet with Senior Leadership Team to regularly discuss incidents and developments Coordinate work with the school's Designated Safeguarding Lead and Deputy Safeguarding Lead
Teaching and Support Staff	Participate in any training and awareness raising sessions Read, understand and sign the Staff Acceptable Use Policy Act in accordance with the Acceptable Use Policy and online safety Policy Report any suspected misuse or problems to the online safety Leader Monitor ICT activity in lessons, extracurricular and extended school activities
Pupils	Read, understand and sign the pupil acceptable use policy and the agreed class internet rules. Participate in online safety activities. Report any suspected misuse to an adult
Parents and Carers	Discuss online Safety issues with their child(ren) and monitor their home use of ICT systems including mobile phones, age restricted apps and games devices Keep up to date with issues through newsletters Inform the Headteacher of any online safety issues that relate to the school
Technical Support Provider	Ensure the school's ICT infrastructure is as secure as possible Ensure users may only access the school network through an enforced password protection policy for those who access children's data Maintain and inform the Senior Leadership Team of issues relating to filtering Keep up to date with online Safety technical information and update others as relevant Ensure use of the network is regularly monitored in order that any misuse can be reported to the online safety Leader for investigation Ensure monitoring systems are implemented and updated Ensure all security updates are applied (including anti-virus and Windows)

ONLINE SAFETY POLICY

Online safety encompasses the use of new technologies. 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 online experience.

THE CORE ONLINE SAFETY POLICY

This online safety policy provides the essential minimal school online safety policy.

The schools online Safety Guidance is available on South West Grid for Learning (SWGfL) and North Somerset website provides further information on online safety issues and links to further information.

END TO END ONLINE SAFETY

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through publicised policies
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband from the South West Grid for Learning Consortium including the effective management of the filtering and monitoring system
- National Education Network standards and specifications. Further Information: http://www.swqfl.orq.uk/Staying-Safe

WRITING AND REVIEWING THE ONLINE SAFETY POLICY

- The school will appoint an online safety leader – Nicola Gee
- Our online safety policy has been written by the school, building on the South West grid for Learning Online safety Policy and government guidance. It has been agreed by Senior Management and approved by governors
- The online safety Policy and its implementation will be reviewed annually
- The online safety Policy was revised by: Nicola Gee October 2023
- The e-safety governor is: Carol Motteram
- It was last approved by the Governors as per the signature on the last page

TEACHING AND LEARNING

WHY INTERNET USE IS IMPORTANT

- 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

INTERNET USE WILL ENHANCE LEARNING

- 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
- 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

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 LA advisors and with the South west Grid for Learning

Children emails

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Any incidents will be recorded
- 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
- Pupils have been advised to only open attachments from known and safe sources or to check with the teacher if in doubt

Staff emails

- Staff will only use official school email addresses to communicate with parents or children
- Staff will sign the schools Acceptable use policy annually

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 Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing pupils' images and work

- Photographs that include pupils' full names will not be used anywhere on the website particularly in association with photographs
- Photos will not be uploaded to social networking sites by school staff and is actively discouraged by anyone else, including pupils and parents, without full permission of all the people in the photograph

Social networking and personal publishing

- The school will block/filter access to social networking sites
- Pupils will be advised never to give out personal information of any kind which may identify them or their location
- Pupils will be advised of the possible risks that the use of social network spaces outside school, primary aged pupils can be exposed to as part of their online safety lessons
- Staff will be advised of appropriate use of social networking sites
- This will be part of the Acceptable Use Policy (APU) that all staff will sign annually (see attached appendix) and also the Social Media Policy

Managing filtering

- The school will work with the LA, DfES 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 an adult, who will consult the online safety Leader

- St Andrews Primary School IT Support and the Computing Lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

Managing emerging technologies

- Emerging technologies will be examined for educational benefit before use in school is allowed

POLICY DECISIONS

Authorising internet access

- All staff must read and sign the "Acceptable ICT Use Agreement" before using any school ICT resource. They will be required to sign it on an annual basis
- The school will keep a record of all staff and pupils who are granted Internet access The record will be kept up to date, for instance a member of staff may leave or a pupils access be withdrawn
- Parents will be advised of the online safety rules and have access to the online safety policy through the school office and the school website

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 North Somerset 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 online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff/head teacher
- Any complaint about staff misuse must be referred to the Head teacher

Community use of the Internet

- The school will advise members of the community using the schools Internet that they will need to abide by the school online safety rules as displayed in the suite
- Any misuse and they will have access withdrawn

COMMUNICATIONS POLICY

Introducing the online policy to all pupils

- Online safety rules will be posted in all classrooms and discussed with the pupils when appropriate
- Pupils will be informed that network and Internet use will be monitored
- Pupils will be informed that cyber-bullying will not be tolerated in or out of school Any complaints will be investigated and pupils and parents will be informed of any actions taken in cases raised
- These will be recorded and kept by the Head teacher.

Staff and the online safety policy

- All staff will be given the School online safety Policy and its importance explained
- Staff will sign an Acceptable Use Policy annually

Enlisting parents' support

- Parents' attention will be drawn to the School online safety policy in newsletters and on the school website
- Adults working with pupils using the Internet will be made aware of the School online safety Policy

MOBILE PHONES AND OTHER DEVICES

Children

- Children should not access mobile phones/devices during the school day and/or on school premises
- Any mobile phone/device will be handed in to the class teacher and placed in the class box at the beginning of the school day and handed back at the end of the school day
- Mobiles are stored in the school office

Staff and Adults in School

- Staff will not use any mobile phone/device where children are present
- Mobile phones will need to be locked away in staffroom lockers or in lockable classroom cabinets

ONLINE SAFETY AUDIT

- St Andrew's Primary School have signed up to the 360 safe audit which is an online self-review tool
- This will be regularly updated and added to by the online safety lead

To be read in conjunction with:

- Staff and Pupil Acceptable Use agreements
- Social, Media and Networking Policy
- Computing Policy
- Behaviour Policy/Peer on Peer Policy
- GDPR
- PSHE
- Inclusion Policy
- Health and Safety Policy

Policy Review

• This policy will be reviewed by the Curriculum Subject Leader annually or more regularly in the light of significant new developments in the use of technologies, new threats to online safety or incidents that have taken place. And every three years by the Curriculum & Staffing committee.

Subject Coordinator:	Nicola Gee
Governor Signature:	(going for ratification Feb 2024)
Review Date:	01/10/2024