Online Safety Policy

Overview

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteacher's and school staff.
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation in schools

The policy also takes into account the National Curriculum computing programme of study.

Online Safety encompasses Internet technologies, electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguarding and awareness for users to enable them to control their online experience. This policy has been revised to reflect the need to raise awareness of the safety issues associated with electronic communications. This Online-Safety Policy operates in conjunction with other policies including those for Computing, Behavior and relationships, Relationships and Sex Education RSE and health education, Safeguarding and Child Protection, all which can be found on the policy section of the school website.

Aims:

It is our aim at St William's Catholic Primary School and Nursery to recognise the importance of e-learning and the significant benefits presented to pupils, staff and parents by the emerging technologies used at home, at school and in the workplace. As a school we also understand the significant risks inherent in the use of these technologies and this policy aims to minimise these risks by:

- Ensuring all staff are aware of the responsibility they have and clearly understand their roles and duties in delivering a high-quality online safety scheme which educates all pupils in how to stay safe online.
- Ensuring a consistent whole-school approach to the teaching of E-safety using National Online Safety which covers the 8 topics outlined in the IKCIS Education for a Connected World Framework (Self-image & identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, wellbeing and lifestyle, Privacy and security, Copyright and ownership).
- Providing a framework for the handling of online safety incidents.

Roles and responsibilities Governors

The governing board has responsibility for reviewing and monitoring this policy. The governor who oversees online safety is **Mrs Clements** as Safeguarding governor**,** supported by **Mr** Lang as computing governor. Governors may ask to see a copy of the filtering and monitoring reports via the headteacher, **Mrs Hogarth**

All governors will review this policy annually and as necessary in response to any online safety incidents to ensure the policy is kept up to date and covers all aspects of technology use within the school. It is their responsibility to keep up to date with emerging risks and threats through technology use and discuss with the Head during committee meetings.

Headteacher

The Headteacher has overall responsibility for online safety within the school and will:

- Ensure that staff understand this policy, and that it is being implemented consistently throughout school.
- Ensure all staff have had appropriate online safety training and professional development.
- Deal with online safety incidents promptly and appropriately
- Allocate necessary resources to the teaching of online safety.

The Designated Safeguarding Lead (DSL)

Details of the school's DSL (and deputy DSL), are set out in our safeguarding policy which can be found on our school website. It is their responsibility to:

- Work alongside the Headteacher and computing subject leader to ensure staff understand this policy and this it is being implemented consistently across school.
- Work with the Headteacher and other staff, as necessary, to address any online safety issues or incidents in line with the schools Safeguarding and Child Protection policy.
- Ensure any incidents relating to online safety and cyber-bullying are logged following the schools safeguarding protocols and dealt with in line with the Safeguarding policy.
- Update and deliver staff training in regard to online safety and safeguarding.
- Liaising with other agencies and/or external services if necessary.

The IT Technician

The IT technician, contracted by the Remedian, is responsible for ensuring the schools IT technical infrastructure is secure, fit-for-purpose and kept up to date. Working alongside the Headteacher, the IT technician will:

- Put into place appropriate levels of security protection procedures, such as filtering and monitoring systems and password protection.
- Ensure that the schools IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Block access to potentially dangerous sites, and where possible, prevent the downloading of potentially dangerous files.

All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently across school.
- Agree and adhere to the schools acceptable use of the schools ICT systems and the internet, and ensure pupils follow the schools terms on acceptable use.
- Work with the DSL and Headteacher to ensure any online safety incidents are logged and dealt with appropriately in line with this policy and the schools Safeguarding policy.

Parents

The school recognises that emerging technologies present significant challenges to parents who often have questions or concerns about online safety. The school aims to work alongside parents and provide them with the latest new and emerging online risks. Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Notify a member of staff or the Headteacher of any online safety issues that arise regarding their child.
- Ensure their child understands acceptable use of the school's ICT systems and internet use and regular reminds and supports their child of appropriate online use.
- Work alongside class teachers to ensure online safety messages are continued to be embedded at home.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- National Online Safety
- Childnet International
- NSPCC – Keeping children safe online
- Gov.uk – Child safety online, A practical guide for parents and carers
- UK Safer Internet Centre

Teaching and Learning Why Internet use is important

The internet is an essential element in modern life for education, business and social interaction. It provides new opportunities for young people's learning and growth, but it can also expose them to new types of risks. At St William's Catholic Primary School and Nursery we have 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 purpose of internet use in school is to raise educational standards, promote pupil achievement, support the professional work of staff and to enhance the school's management functions. Accessing the internet is becoming more accessible for children and young people. Our role as educators is to ensure children learn how to evaluate internet information and to take care of their own safety and security.

How internet use will enhance learning

Our school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use within school. Internet access is planned to enrich and extend learning activities. Access levels can be reviewed to reflect the curriculum requirements and age of pupils.

Staff will ensure learning outcomes are planned around the pupils' age and maturity using the National Online Safety scheme. Pupils will also be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Before using a new device or an online learning resource, pupils will be taught how to use it safely and appropriately.

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. Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work. Using the internet will not be restricted to computing lessons and will be used across our wide-ranging curriculum. This will help us to educate our pupils and further embed key messages about online safety whilst searching the internet.

National Online Safety

Being online is posing an ever-increasing risk to children and it is important that schools, parents and carers work together to take an active role in teaching children about online dangers. National Online Safety has a whole school approach to E-safety with comprehensive training and resources for teachers, parents and children. All staff will be given unique login details to access National Online safety. Parents will also receive guidance and support for creating an account for their child to access at home. The teaching of online safety will be consistent throughout school and of high quality. Pupils will engage in frequent online safety lessons based on the 8 topics outlined in the UKCIS Education for a Connected World Framework:

- Self-image & identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing & lifestyle
- Privacy & security
- Copyright & ownership

Educating Pupils about Online Safety

At St William's Catholic Primary School and Nursery our online safety curriculum is taken from National Online Safety, National Curriculum computing programme of study and Relationships and Sex Education (RSE) and Health Education.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behavior.
- Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, pretending to be someone they are not.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others whilst online.
- How to respond safely and appropriately to online situations with people they may encounter and whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching pupils about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.
Please see our computing overview on the curriculum page of our school website to see how online safety will be delivered across school.

Managing Internet Access Information system security

The schools ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed with Remedian services. Files held on the school's network will be regularly checked. The IT Technician will review system capacity regularly.

E-mail

Pupils may only use approved e-mail accounts on the school system and will only be permitted to access these email accounts under staff supervision. Pupils will be taught to not reveal their personal details or of others in school. Pupils are educated about the dangers of phishing and spam emails. All staff will be given an email address linked to the school. All staff must show respect for all members of the school community by being polite, courteous and refrain from the use of inappropriate language whilst using their school email account.

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

Publishing pupil's images and work online

Written permission from parents or carers will be obtained before photographs of pupils or their work are published on to the school website or Class Dojo. Pupils' full names will not be used on the website or Class Dojo with a photograph. Pupil's work and photographs will only be published on the school website or Class Dojo with the annual permission of the pupil, parent and carers.

Class Dojo

Children will have unique login details to access the safe and secure learning platform, Class Dojo. Staff will ensure login details are kept confidential and parents will be able to attain their child's unique login details from their child's class teacher. Class Dojo is a safe, secure and private

platform to communicate with parents and carers. Parents and staff will be able to communicate via the direct messaging system. Parents will be reminded that the messaging system should only be used for educational subject matter online and during appropriate school hours. Parents have the opportunity to opt in or out of using Class Dojo. Parents will receive guidance and support around using Class Dojo at home. School will obtain written consent before photographs of pupils and their work are uploaded to Class Dojo.
For privacy details, please visit: https://www.classdojo.com/privacy/
For full terms of service, please visit: https://www.classdojo.com/en-gb/terms/

Social networking and personal publishing

The school will block access to social networking sites other than Facebook which is used as a way of communication and for promoting our school. Newsgroups will be blocked unless a specific use is approved. Pupils will be reminded never to give out personal details of any kind which may identify them or their location. Being online is an integral part of children and young people's lives. Social media, online games, websites and apps all form part of their online world. Pupils and parents will be advised that the use of social network platforms outside of school is inappropriate for primary aged pupils. Parents will be made aware of the safety implications for children when using social media and will be encouraged to supervise and monitor their child's internet use at home. As a school we acknowledge the risks social media platforms present, such as cyberbullying, online grooming, emotional abuse and online abuse. At St William's Catholic Primary School and Nursery we will foster an open environment where pupils feel safe to ask questions, engage in conversations and raise any concerns about their online experience.

Managing filtering

The school will work with Remedian, DfES and the Internet Service Provider to ensure our systems to protect pupils are reviewed and improved. Our web filtering service, Fortigate, is put into place by Remedian. This service provides safe, filtered and logged web access for all staff and students using our school's broadband connection. The service provides the following functionality:

- Education focused web filtering
- Different filtering policies and access based on the user, staff or pupil.
- Local control to allow the school to manage which websites and categories of websites we wish to allow or block.
- Meets the DfE recommendations for web filtering to protect pupils online and the standards for schools' web filtering set by the UK Safe Internet Centre.
- Illegal content remains blocked at all times and access cannot be over-ridden by school staff.
- Alerting capabilities. The Headteacher is alerted when a matter of concern is identified in regard to internet use from staff or pupils.
- Generated reports of internet usage of all staff and pupils. The Headteacher can configure and schedule their own reports of internet usage and these reports can be exported for further in-depth analysis.

If staff or pupils discover an unsuitable site, it must be reported to the Headteacher and reported in the schools IT recording and monitoring book. Senior staff and the schools IT technician will ensure

that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing

Video conferencing will be appropriately supervised for the pupils' age. Staff using video conferencing for the purposes of communication outside of school, such as an enforced period of self-isolation as a result of COVID-19, will ensure an adult is present when conversing with a pupil. Staff using video conferencing to communicate with an external service or educator should use the schools broadband network to ensure quality of service and security.

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.

Mobile phone use

The use of personal electronic devices, including mobile phones and cameras, by staff and pupils is closely monitored by the school, in accordance with the Staff Code of Conduct and Staff Handbook. The use of mobile phones by staff and visitors is restricted to areas of school not occupied by pupils and restricted to times when staff in school are not timetabled to be working with children. In almost all circumstances, other than for medical or emergency reasons, staff should only access their personal devices during their break times.

Staff will report any concerns about pupils' or other staff members' use of personal electronic device to the DSL, following the appropriate procedures. St William's Catholic Primary School and Nursery is committed to keeping pupils safe by ensuring that electronic devices such as cameras, phones and tablets are used in an appropriate manner.

Staff must ensure that:

- Parental/career consent is obtained to take and use photographs and/or videos of children, for use in school, to market the school or to share on the school website. Any photos taken of children during the school day, with parental/career consent, need to be deleted as soon as possible and before the end of the school day.
- Communication between pupils or parents is made on the school telephone and not their personal electronic device unless in unavoidable circumstances.
- Visitors, volunteers and students do not use their personal electronic device to take or record any images of children.

While we acknowledge a parent's right to allow their child to bring a mobile phone to school for travel purposes e.g. if they walk to and from school without adult supervision, St William's Primary School discourages pupils bringing mobile phones to school due to potential online risks. When a child needs to bring a phone into school, the mobile must be left in the school office at the start of the day and collected at the end of the day. Parents are advised that school accepts no liability for the loss or damage to mobile phones which are brought into school or school grounds.

Children that need mobile devices for medical reasons will be allowed to have them in school, but will have limited access to them during the school day.

Where a pupil is found by a member of staff using a mobile phone during the school day, the phone will be confiscated from the pupil, and handed to the Headteacher or a member of the school office team. The pupil may then collect the mobile phone at the end of the school day and will be reminded of our schools mobile phone use. Should a pupil be found using their mobile phone inappropriately, the school reserves the right to withdraw this privilege and the Headteacher will decide the appropriate course of action. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. Should parents need to contact pupils during the school day, this should be done via the school office phone or email.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Please see our data protection policy on our school website.

Handling online-safety complaints and misuse

Where a pupil misuses the school's ICT systems or internet, the Headteacher will decide the appropriate course of action. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. Where a staff member misuses the schools ICT systems or the internet, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. Pupils are encouraged to report any online safety concerns with a member of staff in school or an adult at home. All staff have a duty to report any concerns in line with the schools incident recording procedures set out in the Safeguarding policy. Complaints of Internet misuse will be dealt with by a senior member of staff and Headteacher. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a safeguarding nature must be dealt with in accordance with schools safeguarding procedures.

Introducing the Online-Safety policy to pupils

Online-safety rules are posted in all rooms with Internet access and are discussed with pupils at the start of each year. This is reviewed termly to ensure our pupils have a secure understanding of online risks and how to stay safe. Pupils will be reminded that network and internet use is monitored within school using our schools filtering and monitoring system. Our online-safety scheme, National Online Safety is followed across school to raise the awareness and importance of safe and responsible internet use. Online-safety modules are also included in our PSHE scheme of learning, SCARF, which covers both school and home use. We have a whole school approach to online safety and take part in Online Safety day each year to ensure the teaching of key messages is consistent.

Remote Learning

Using the internet at home:

We can only be successful in keeping children safe online if we work with parents to ensure the e-safety message is consistent in school and at home. Parental support is needed to guide children to know and understand what appropriate online behavior is. Online safety can be daunting for

parents and careers, as they may have concerns about their understanding of the topic and their knowledge. Support and guidance will be given to parents through the sharing of resources and policies on our school website and Class Dojo. We will encourage parents and careers to maintain an open and ongoing discussion about online safety at home, as a family, with their children. Online safety concerns should always be reported to the child's class teacher. Parents can do this through Class Dojo messaging or by phoning the school office. We will work closely with parents to resolve any concerns in line with our behaviour and relationship policy.

Whilst learning at home, pupils will only be expected to use high quality online educational resources, appropriate to their age and ability such as:

- Time Table Rockstars (TTS)
- Numbots
- Rollama
- ActiveLearn

All pupils have been issued with unique login details to support their learning whilst at home. Staff will use these resources to set appropriate home learning tasks. Pupils are reminded that these platforms are monitored by staff. For more guidance about these educational resources, please speak with your child's class teacher.

Policy date: September 2025
Update due: September 2026