

**Online Safety Policy**

**2023**

**Aims of the School**

1. The school aims to show concern, in a school that looks to Christ for the basis of its existence, for all the teaching staff together with all the non-teaching staff and parents, as well as the pupils.

2. The school aims, through prayer, worship and liturgy, to develop the Faith of each individual in the school community.

3. The school aims to ensure that the curriculum provides a Catholic Christian setting in which the children can grow in Faith and understanding and in the acquisition of skills, attitudes, values and knowledge.

4. The school aims to prepare the pupils to become active and responsible within the home, school, parish and the wider community in which they may live.

**Mission Statement**

At St. Anthony’s we believe we are a community striving to live, love and learn together joyfully following Jesus Christ.

**St. Anthony’s Catholic Primary School Online Safety Policy**

Our Online Safety Policy is a working document which has been written using Government and Local Authority Guidance. It has been tailored to reflect our school community and has been agreed by the senior management and approved by governors.

The policy and its implementation will be reviewed regularly.

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 functions. 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. The school has a duty to provide students with quality and safe Internet access as part of their learning experience.

Pupils use the Internet widely outside of school and will need to be taught how to evaluate Internet information and take care of their own safety and security online.

This policy applies to all members of the school community who have access to and are users of school ICT systems both in and out of school. The aim of this policy is to ensure that all are aware of the safety issues associated with information systems and electronic communications. Its purpose is to allow all members of the community to enjoy the many benefits of electronic communication whilst understanding the dangers and taking appropriate precautions to keep themselves (and others) safe.

The Online Safety Policy relates to other policies in school Safeguarding. The school will deal with such incidents within this policy and will, where known, inform parents/carers of incidents of inappropriate online behavior that takes place outside of school.

The Online Safety Co-ordinator is Kieran Scanlon.

**The Online Safety Co-ordinator (alongside senior leadership and IT support) are responsible for:**

* Day to day responsibilities for online safety issues.
* Leading, establishing and reviewing the Online Safety Policy and relevant documents.
* Ensuring all staff are aware of the procedures which need to be followed in the event of an online safety incident.
* Ensuring that guidance is provided to staff which is read and understood and that this guidance is part of the training for new staff at the school at any point in the academic year.
* Liaising with the Local Authority and any other relevant bodies.
* Attending relevant Governors Meetings.
* Reporting regularly to Senior Leadership.

**Teaching and support staff are responsible for ensuring that:**

* They have an up-to-date awareness of Online Safety and the current school Online Safety Policy and practices and their professional responsibilities in line with this.
* They report and share any issues, concerns or suspected misuse to relevant staff for further investigation.
* They report any unsuitable sites or content not picked up by our filtering/monitoring system (Smoothwall) to the Head Teacher who will report it to SMBC Education ICT Services.
* Any digital communications they have should be on a professional level and only carried out using official school systems.
* Online Safety teaching is embedded across the curriculum.
* Pupils understand and follow the Online Safety Policy.
* Internet use is pre-planned where possible, ensuring pupils are directed to sites which have been checked and deemed suitable for their use.
* Pupils have a good understanding of how to research, avoiding plagiarism and upholding copyright regulations.
* They follow relevant processes for dealing with any unsuitable material that is found in internet searches.
* When personally using the internet, for example for social media, they ensure the maximum privacy settings are used and that they will not discuss the school, parents or pupils.

**Pupils are responsible for ensuring that they:**

* Follow teaching, guidance and instruction given when using digital technology systems in school.
* Follow guidance and understand the importance of reporting abuse, misuse or any inappropriate materials they may come across.
* Understand that the school’s Online Safety Policy covers their actions outside of school, if related to their membership of the school.

**Parents**

Parents will be supported by school to ensure they understand their crucial role in ensuring their children understand how to keep themselves safe online and when using technology. Online Safety issues will be raised and brought to their attention via newsletters, letters, emails, sharing website links, tweets, parent workshops and signposting to relevant help organisations.

Parents will be encouraged to support the school and follow guidelines on the appropriate use of digital and video images taken at school events (see Digital and Video Images section).

**The Curriculum**

Online Safety is an essential part of the curriculum. Pupils need to be taught how to recognise and avoid online safety risks and know what to do should they need help with online issues. Online Safety should be taught through all areas of the curriculum (including RSE) and staff should reiterate the importance of these messages. Online Safety teaching needs to be up-to-date, relevant, age-appropriate and engaging. It will include teaching on:

* Safe and appropriate use of mobile technologies both within and outside of school.
* Acceptable use of the Internet.
* Knowing online use in school (and in some cases outside of school) is monitored and can be traced.
* Awareness of not giving out personal information including passwords or any other information which may identify them or their location.
* Being critical of online materials and content and considering the accuracy of this information.
* Acknowledging sources of information.
* Understanding the importance of reporting abuse, misuse and inappropriate materials and how to do so.

School will take part in Safer Internet Day, assemblies, workshops and other relevant events to boost engagement and Teaching and Learning around Online Safety.

Pupils will be encouraged not to use Social Networking sites until they are legally old enough to do so.

**Internet Access**

* All staff and pupils are granted Internet access, although access could be denied in the event of inappropriate use.
* In EYFS, pupils are only able to access the sites and software specifically designed for their needs following adult demonstration and with adult supervision.
* In KS1 and KS2, access to the Internet is preceded by adult demonstration with direct supervision. These opportunities are pre-planned, directed and safe, specific, approved sites are used.
* Smoothwall operates so that users access the Internet having first logged in using their individual username and password and therefore their internet use can be monitored.
* Pupils have access to The Big Red Button and are taught to use this should they see any unsuitable material on a computer in school and then report the incident to a member of staff immediately.
* 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 device connected to the school network. Neither the school nor SMBC can accept liability for the material accessed, or any consequences of Internet access.

**Digital and Video Images**

* Staff should inform and educate pupils on the risks associated with taking, using, sharing, publishing and distributing images. This should include publishing their own images on the internet.
* Written permission is obtained from parents/carers before photographs of the children are used on the school website/newsletters/Twitter and any external events. This information will be collected each academic year.
* Staff will only use iPads and tablets owned by and registered to the school to take photographs of the children unless special permission sought from Head Teacher.
* Parents/carers are allowed to take digital images and videos of their children at certain school events for their own personal use. For Safeguarding purposes, parents/carers are not allowed to upload photographs or videos that they take of any school event onto the Internet. They are explicitly reminded of this at each school event that takes place.
* Pupils full names will not be used anywhere on the school website or school communications, particularly in association with photographs.
* The use of video conferencing will be appropriately supervised for all pupils.

**School Website**

* The Head Techer will take overall editorial responsibility for the school website and ensure the content is accurate and appropriate.
* Photographs which include pupils will be carefully selected.
* Staff images will be published with consent.
* Staff or pupils personal information will not be published.

**Email**

* Incoming emails should be treated as suspicious and attachments not opened unless the author is known.
* The forwarding of chain letters is not permitted.

**Telephone**

* Where possible, calls to children/parents/carers will be made from school telephones.
* When this is not possible, staff will use 141 before dialing so as not to share their personal telephone numbers.

**Devices**

* Mobile phones and wearable devices will not be used during lessons or formal school time by staff.
* Children should not wear wearable devices which have a camera to school.
* Only children in Year 6 who require a mobile phone due to walking home alone are permitted to bring a mobile phone to school. Mobile phones must be given in to the school office at the beginning of the day and collected at the end of the day.
* Staff should only use iPads and tablets for information relating to school use.

**Home Learning**

* Use of any online learning tools and systems will be in line with privacy and data protection requirements.
* All procedures and expectations set out in this policy will continue to be adhered to.
* The majority of Home Learning will be set using Microsoft Teams which is a secure, authenticated platform for which children have unique logins.
* Where children are directed to other websites, staff will check suitability of content in advance.
* If videoing themselves, staff will be conscious of ensuring videos are suitable e.g. using professional language, wearing suitable clothing, being mindful of backgrounds etc.

**School Security**

* The security of the school information systems will be reviewed regularly.
* Virus protection will be installed and updated regularly (Solihull MBC).
* School uses Solihull Broadband with its firewalls and filters.

**Filtering and Monitoring**

* The school will work in partnership with Solihull EICTS Development Service to ensure filtering and monitoring systems continue to be as effective as possible.
* Senior leadership will ensure that regular checks are made to ensure filtering is appropriate, effective and reasonable.
* School currently uses ‘Smoothwall’ filtering and monitoring.
* The filtering system automatically checks all content, supporting the ‘Keeping Children Safe in Education 2022’ document.
* The monitoring system reports on all internet use, and these reports help to identify potential safeguarding issues – including potential misuse by staff – so that these issues can be investigated by school leaders.
* Staff and pupils are aware of monitoring which takes place.
* The Head Teacher receives usage reports and investigates potential misuse if thought to be a breach of school policy.

**Online Safety Complaints**

* Complaints of internet misuse will be dealt with by a senior member of staff.
* Any complaints of staff misuse must be reported to the Head Teacher.
* Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
* Incidents of potential bullying will be dealt with in line with school’s policy on bullying.

**Data Protection**

* Personal data will be recorded, processed, transferred and made available according to the school’s Data Protection Policy.
* Memory sticks and laptops must be encrypted.
* Staff and pupils are made aware that they must not give their username and password to any other individual.