St. Anne's Catholic Primary School

Online Safety Policy

Our School Mission Statement:

Each one of us is special
Each one of us is unique
Because we are created by God's love
May God's love shine on our lives
As we care and share and learn together

Introduction & Aims

This Online Safety Policy has been designed and created by stakeholders at St. Anne's Catholic Primary School. It is a working document, which (in line with Government and Local Authority documentation) has been tailored to reflect our school community and the vision of our school.

As a Catholic school, we believe that Christ is at the centre of everything that we do. Our ethos is driven by the Gospel values, where we encourage and guide the children in our care to be more like Jesus every day. Our School Mission Statement identifies that we are all unique and special, made in the image of Jesus Christ. It is through this that we recognise each child as a member of God's family where they are valued, respected and cared for.

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) 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 our community to enjoy the many benefits of electronic communication whilst understanding the dangers and taking appropriate precautions to keep themselves 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 Safety behaviour that takes place out of school.

The online safety co-ordinator is Mr Linehan (Head-teacher and Lead DSL). Our Online Safety Policy has been written by the school, building on guidance from Our Lady & All Saints Multi-Academy Company.

The online safety co-ordinator (alongside support from the Head Teacher and Technician):

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Ensure that guidance provided to staff is read and understood and that this document is part of the training for new staff starting the school at any point in the academic year
- Liaises with the Local Authority/relevant bodies
- Attend relevant Governors meetings
- Report regularly to SLT.

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety policy and practices
- They report any suspected misuse or problems to the relevant staff for investigation
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the online safety and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Staff to share any concerns via Online Safety Co-ordinator and DSLs in school, sharing any concerns via CPOMs. Students/Pupils are responsible for:

- Using the school digital technology systems in accordance with the Parent Acceptable Use Agreement
- Having a good understanding of research skills and the need to avoid plagiarism
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Understanding the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

- Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.

The school will take every opportunity to help parents understand these issues through newsletters, letters, website links, parent workshops and information about national campaigns. 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.

For Safeguarding purposes, parents/carers are not allowed to upload photographs or videos that they take of any school event onto the internet (Twitter/Facebook etc.). They are explicitly reminded about this at school events e.g. assemblies, productions etc. in order to comply with our Safeguarding arrangements. We thank our parents/carers for their cooperation with this matter.

Online safety through the curriculum

The education of pupils in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum (including RSE) and staff should reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- Pupils should be taught in lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of this information

- Pupils will be taught about acceptable Internet use and which Internet use is acceptable and given clear objectives for Internet use

- Pupils will understand that their use will be monitored and can be traced back to the user through their username

- Pupils should be taught to acknowledge the source of information, where appropriate.

- Pupils should be supported in building resilience to radicalisation

- Pupils should be taught about the safe and appropriate use of mobile technologies, and as a staff we must strive to keep up to date with new technologies

- Pupils should be helped and encouraged to adopt safe and responsible use both within and outside school

- Safer Internet Day (typically every February each year) will be an active source of Teaching & Learning

- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.

- Pupils will be encouraged not to use Social Networking sites until they are legally old enough. If staff or pupils discover unsuitable sites or content this must be reported to the Head Teacher who will report it to the SMBC EICTS (Education ICT services) team. This is alongside the use of our filtering/monitoring system (Smoothwall).

Staff responsibilities for Online Safety

- All staff and pupils are granted Internet access, although access could be denied in the event of inappropriate use

- In the Early Years Foundation Stage pupils are only able to access the sites and software specifically designed for their needs following adult demonstrations

- At Key Stage 1 & 2, access to the Internet and Extranet will be by adult demonstration with directly supervised access to specific, approved on-line materials (safe searches)

- 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 SMBC can accept liability for the material accessed, or any consequences of Internet access. E-Mail. Children understand that if they see unsuitable material on a computer in school, they must click on the red "Oh No!" link to report it immediately.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites

- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website/social media/local press. Each academic year a reminder regarding this consent will be in the school newsletter, and if parents wish to change they must inform us

- If a child's photograph is not allowed to be published then this information will be kept centrally and shared with staff that support that child.

- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection these images should not be published nor should parents/carers comment on any activities involving other pupils in the digital images. Parents/ carers are regularly reminded of this at each event that takes place.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such image

- Pupils full names will not be used anywhere on a website or blog, particularly in association with photographs

- The contact details on the web site should be the school address, email 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

- The security of the school information systems will be reviewed regularly

- Virus protection will be installed and updated regularly (Solihull M.B.C.)

- The school uses the Solihull Broadband with its firewall and filters.

Managing filtering and monitoring

- The school will work in partnership with the Solihull EICTS Development Service to ensure filtering and monitoring systems continue to be as effective as possible

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

- We currently use 'Smoothwall' as the filtering and monitoring system in line with Keeping Children Safe in Education (KCSIE) '24.

- The filtering system automatically checks all content including content that was not previously checked. This supports the 'Keeping Children Safe in Education 2024 document

- The monitoring system reports on all internet use, and these reports will identify potential safeguarding issues and behaviour issues – including potential misuse by staff – so that these issues can be investigated by school leaders

- The Head Teacher receives usage reports as a result of this. Any potential misuse detected could be investigated by the school if it was thought to breach the school's policies. Handling online safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff

- Any complaint about staff misuse must be referred to the Head Teacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures

- Data Protection: Personal data will be recorded, processed, transferred and made available according to the Schools Data Protection Policy (in accordance with the relevant Data Protection laws, including the General Data Protection Regulations)

Information provided to staff:

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communication systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's.
- I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person
- I will report any incidents of concern regarding children's safety to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems
- I will not access, copy, remove or otherwise alter any other user's files, without their permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school online safety, social media and mobile devices policies
- Where images are published (E.g. on school website) it will not be possible to identify by name, or other personal information who is featured.)
- I will only use social networking sites in school in accordance with the schools policies
- I will only communicate with pupils and parents/carers using official school systems and any such communication will be professional in tone and manner
- I will not engage in any online activity that may compromise my professional responsibilities. The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school

- When I use my mobile devices in school (laptops, tablets, phones) I will follow the rules set out in this agreement and the Mobile Devices Policy, in the same way as if I was using school equipment.

Alongside the Online Safety, Social Media, and Mobile Devices Policy, please also note:

- KS1 + 2 staff must store phones away from children to ensure they are not accessible by children
- Where possible mobile phones should have a password secured keypad
- I will not use personal email addresses on the school ICT systems
- I will not open any hyperlinks in emails or any attachments to emails unless the source is known and trusted
- I will ensure that my data is regularly backed up, in accordance with school policies
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the schools filtering/security systems
- I will not install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings unless I have been given permission
- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original works of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music/videos)
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing in accordance with the curriculum plans

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage

- The school may exercise its right to monitor the use of the schools information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing of unlawful text, imagery or sound

This Policy was reviewed and agreed by staff: Autumn '24
Review date: Annually