St. Antony's Catholic Primary School

Acceptable Use and On-line Safety Policy

Learning Together In God's Love

Reviewed by staff: Autumn 2024
Agreed by Governors: Autumn 2024
Review date: Autumn 2026

Introduction and Policy Statement

Ethos

Our Catholic ethos is embedded in all aspects of school life as we place Christ central to what we do and are influenced by the Core Christian Principles which underpin every policy and procedure which guide our day to day practice. Keeping our children safe at St Antony's is encapsulated in our Mission Statement and in our Philosophy and Overarching Aims for the school.

Our Mission Statement

At St. Antony's Catholic School we celebrate our special talents as children of God:

1. ***We try to be like Jesus and always keep Him in our hearts.***
2. ***We work together in our homes, school and parish to share our gifts and learn together.***
3. ***We understand that we are all different and we respect each other regardless.***
4. ***We look after our world so that we may share it together in peace***

As by doing all these we ensure that we are all 'LEARNING TOGETHER IN GOD'S LOVE' each day

Philosophy/Overarching Aim

As a school family our aim is to make a real difference in our children's lives. We believe that **Keeping Children Safe in Education** runs central to all the work that is done towards raising our children's overall educational achievement. If a child is safe, valued, well cared for and protected from maltreatment and neglect along with having their human rights secured then this is fundamental towards improving their future quality of life and by extension their families'. We are determined to ensure that all our children are not only safe in education but we also aim to eradicate the impact and stigma of low expectations regarding educational standards and achievement that are rife in the wider local community. We aim to do this by acknowledging and challenging the impact of disadvantage and discrimination in all forms that exist around the pupils under our care.

All schools and their staff inclusive of ours, form part of the wider safeguarding system for children. Everyone who comes into contact with children and their families and carers has a role to play in safeguarding children. In order to fulfill this responsibility effectively, all professionals working in or with our school should make sure their approach is child-centered. This means that they should consider, at all times, what is in the best interests of the child. (Keeping Children Safe in

Aims

This Online Safety Policy outlines the commitment of St Antony's Catholic Primary School to Safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as reference below.

This Online Safety Policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed). St Antony's Catholic Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 headteachers and school staff
- [Relationships
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so

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

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity (access logs are in the LGFL support portal) • surveys/questionnaires of:
- Learners
- Parents/careers
- Staff

Policy and Leadership Responsibilities
To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals1 and groups within the school.

Head teacher and Senior Leadership Team
• The head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Leaders.

• The head teacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

• The head teacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

• The head teacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

• The head teacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead. (DSL)

Governors
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
This review will be carried out by St. Antony's school governors, whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:
• Regular meetings with the DSL
• Regularly receiving (collated and anonymised) reports of online safety incidents
• Checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
• Reporting to relevant governors group/meeting
• Occasional review of the filtering change control logs and the monitoring of filtering logs (where possible) The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead

The Online Safety Lead will:
• Lead the Online Safety Group
• Work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
• Take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
• Have a leading role in establishing and reviewing the school online safety policies/documents
• Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
• Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
• Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
• Receive reports of online safety incidents and create a log of incidents to inform future online safety developments
• Provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
• Liaise with (local authority/MAT) technical staff, pastoral staff and support staff (as relevant)
• Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
• Attend relevant governing body meetings/groups
• Report regularly to head teacher/senior leadership team.
• Liaises with the local authority/MAT/relevant body
This list is not intended to be exhaustive.

Designated Safeguarding Lead (DSL)
The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:
• sharing of personal data

• Access to illegal/inappropriate materials

• Inappropriate online contact with adults/strangers

• Potential or actual incidents of grooming

• Curriculum Leads will work with the Online Safety Leaders to develop a planned and coordinated online safety education program.

This will be provided through:

• RHSE programs

• Assemblies and pastoral programs

• Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff
School staff are responsible for ensuring that:
• They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices

• They understand that online safety is a core part of safeguarding

• They have read, understood, and signed the staff acceptable use agreement (AUA)

• They immediately report any suspected misuse or problem to the designated safeguarding leads for investigation/action, in line with the school safeguarding procedures

• All digital communications with learners and 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

• Ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices

• In lessons where internet use is pre-planned learners 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

• Where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource

• Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.

• They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Technical Staff

The network manager/technical staff is responsible for ensuring that:

• They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy

• The school technical infrastructure is secure and is not open to misuse or malicious attack

• The school meets (as a minimum) the required online safety technical requirements as identified by the local authority/MAT or other relevant body

• There is clear, safe, and managed control of user access to networks and devices

• They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

• The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the designated safeguarding leads for investigation and action

• The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person

• Monitoring software/systems are implemented and regularly updated as agreed in school policies Learners

• Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed)

• Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• Should know what to do if they or someone they know feels vulnerable when using online technology

• Should understand 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.

Pupils

• Are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed)
• Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• Should know what to do if they or someone they know feels vulnerable when using online technology
• Should understand 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 and Carers

The school will take every opportunity to help parents and carers understand these issues through:
• Publishing the school Online Safety Policy on the school website

• Providing them with a copy of the learners' acceptable use agreement

• Publish information about appropriate use of social media relating to posts concerning the school
• seeking their permissions concerning digital images, cloud services etic

• Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

• reinforcing the online safety messages provided to learners in school

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

• What are the issues? – UK Safer Internet Centre

• Hot topics – Childnet

• Parent resource sheet – Childnet

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

The School Online Safety Policy:

• Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication

• Allocates responsibilities for the delivery of the policy

• Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours

• Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world

• Describes how the school will help prepare learners to be safe and responsible users of online technologies

• Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms

• Is supplemented by a series of related acceptable use agreements

• Is made available to staff at induction and through normal communication channels

• Is published on the school website Acceptable use The Online Safety Policy and acceptable use agreements define acceptable use at the school.

The acceptable use agreements will be communicated/re-enforced through:

• Responsible internet use agreement (distributed to and signed by parents/carers)

• Staff induction

• Communication with parents/carers

• Built into education sessions

• School webs

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors).

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

On-line Safety Guidelines for Children