ST ANSELM'S CATHOLIC PRIMARY SCHOOL

ONLINE SAFETY POLICY

Learning and growing together through prayer, belief and love

This policy was approved by the Pupil Committee of the Governing Body on **10th January 2023** and presented to the full Governing Body on **1st February 2023.**
This policy will be reviewed **annually.**

INTRODUCTION:

At St Anselm's Catholic Primary School, we recognise that online safety in schools is of paramount importance. As the online world evolves, so do both the online harms and risks facing our children and the relevant legislation, both statutory and non-statutory, which directs and guides how schools should meet their online safety requirements.

It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This will support a robust online safety ethos and ensure that schools are providing the best online safety provision they possibly can. The Online Safety policy forms part of our safeguarding suite of policies.

This policy should be read in conjunction with the following policies:

- Whistleblowing
- Anti-bullying
- Acceptable Use
- Behaviour
- Safeguarding and Child protection
- Staff code of conduct
- Staff Low level concerns policy
- Code of conduct for parents, carers and visitors
- Complaints
- Data protection
- Curriculum policies
- Social media
- Mobile phone policy
- Out of School Club Policy and procedures

PURPOSE:

The purpose of this policy is to safeguard and protect all members of St Anselm's online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. The policy is applicable to all members of St Anselm's. This includes staff, students and pupils, volunteers, parents/carers, visitors and community users who have access to and are users of St Anselm's digital technology systems, both internally and externally within the home and community setting.

ROLES AND RESPONSIBILITIES

The following section outlines the online safety roles and responsibilities of all stakeholders across the online community within St Anselm's.

Teachers and Staff

All members of school staff (teaching and non-teaching) have a responsibility to protect children online. This includes every member of staff who works at the school; headteacher, teachers, supply teachers, work-experience staff, office staff, caretakers, cleaners, etc. All teachers and staff must always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All school staff need to:

- Be aware of and adhere to all policies in school which support online safety and safeguarding.
- Contribute to policy development and review.
- Support in the ownership and responsibility for the security of systems and the data accessed.
- Receive appropriate annual child protection and online safety training.
- Be responsible for their own continuing professional development in online safety.
- Model safe and responsible behaviours in their own use of technology.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Know how to recognise, respond and report signs of online abuse and harm.
- Know the process for making referrals and reporting concerns.
- Always act in the best interests of the child.

Governors and Senior Leadership Team

A governor's role for online safety in a school should include, but is not limited to:

- Upholding online safety as a safeguarding issue which is embedded across the whole school culture.
- Ensuring that children are provided with a safe environment in which to learn and develop.
- Ensuring that the school has appropriate filters and monitoring systems in place.
- Ensuring the school has effective policies and training in place.
- Auditing and evaluating online safety practice.
- Ensuring there are robust reporting channels.

Designated Safeguarding Lead (DSL)

With respect to online safety, it is the responsibility of the DSL:

- Ensure teachers and parents are aware of measures to keep children safe online through relevant training provision.
- Take responsibility for all safeguarding matters, including online safety.
- Receive and regularly review Online Safety incident logs and be aware of the procedure to be followed should an Online Safety incident occur in the school.
- Collaborate with the senior leadership team, the online safety lead and computing lead.
- Facilitate effective record keeping and the reporting and monitoring of all online safety concerns.
- Promote online safety and the adoption of a whole school approach.

- Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety through organisations such as Ealing LA, CEOP (Child Exploitation and Online Protection), UKCCIS, and Childnet.

Computing and Online Safety Leads

With respect to online safety, it is the responsibility of the Computing and Online Safety Leads to:

- Promote an awareness and commitment to Online Safety throughout the school.
- Create and maintain policies and procedures.
- Develop an understanding of current Online Safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in Online Safety issues.
- Ensure Online Safety is embedded across the curriculum.
- Ensure Online Safety is promoted to parents and carers.
- Monitor and report on Online Safety issues to the Leadership team, as appropriate.
- Ensure any Online Safety incidents are logged on CPOMs, including a scanned copy of the 'thinking about my behaviour' reflection form, completed by the child.

Technical Staff

With respect to online safety, it is the responsibility of the ICT Technician:

- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school IT systems.
- Report any Online Safety related issues that come to your attention to the Online Safety leader and Senior Leadership Team.
- Develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to your work.
- Liaise with the local authority and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Additional IT support is provided by Wibird for network maintenance and the school's ICT network.

Pupils

With respect to online safety in your school, children need to:

- Know who the DSL and Online Safety Lead is.
- Engage in age appropriate online safety education opportunities.
- Read, understand and adhere the AUP when using computer technology in school.
- Reconfirm agreement of the AUP each time they logon to the school network.
- Respect the feelings, rights and values of others, both off and online.
- Take responsibility for keeping themselves and others safe online including personal technology owned and used by pupils outside of school.
- Know age limitations, guidance and rules regarding social media apps and games.
- Know where and how to find help with any online incidents or concerns.
- Know how, when and where to report concerns and when to seek help from a trusted adult.

Parents and Carers

Parents and carers need to understand the risks that children face online to protect them from online dangers. Parents need to:

- Help and support your child's school in promoting Online Safety.
- Read and adhere to all relevant policies, including Acceptable Use Policy.
- Be responsible when taking photos/using technology at school events.

- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss Online Safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Support online safety approaches and education provision.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if you have any concerns about your children's use of technology.
- Identify changes in children's behaviour that could indicate they are at risk of online harm or abuse
- Know who the school DSL and Online Safety Lead is.
- Know how to report online issues.

TEACHING AND LEARNING

The main online risks to our school community usually fall under one of three categories:

Contact:
Contact from someone online who may wish to bully or abuse the child. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting person information.

Content:
Inappropriate material available to children online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.

Conduct:
The child may be the perpetrator of activities including: illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. Within the National Curriculum computing programmes of study, pupils will be taught to:

Key Stage 1

- 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

Key Stage 2:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour

- 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, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The UKCCIS 'Education for a Connected World' framework aims to equip children and young people for digital life. It covers:

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

At St Anselm’s, we use this to teach online safety and cover at least one of these topics every half term across the whole school to ensure it is progressive. The safe use of social media and the internet will also be covered in other subjects where relevant, for example: RHE or PSHE lessons. The school will use assemblies to raise pupils’ awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. The Online Safety Lead will produce half-termly Online Safety newsletters to further promote online safety, focusing on apps and programmes that are known to be used by the pupils in the school. Digital leaders will be chosen from Years 5 and 6 to help support the Online Safety lead to better understand the needs of the pupils.

Children will be reminded of their responsibility when logging onto the school network and using the internet and will be asked to sign an age appropriate acceptable use agreement (see Acceptable Use Policy appendix 1 and 2). SMART posters will be displayed in all areas where computing equipment is used.

EDUCATING PARENTS ABOUT ONLINE SAFETY

At St Anselm’s, we recognise and cultivate the essential role parents and carers have in fostering safer online safety practices in children and young people. To raise parents’ awareness of online safety, the Online Safety Lead will produce half-termly Online Safety newsletters, publish a weekly ‘Wake Up Wednesday’ guide shared via twitter, and lead an Online Safety workshop annually for Parents.

All information linked to Online Safety is available on the school website, school newsletter, school twitter feed and SharePoint pages. In response to the fast moving development of social media apps, games and websites, any information updates, will be communicated promptly with parents via these channels. In

particular updates regarding social media use will be shared with parents of pupils in Year 5 and 6, as mobile phones have become more popular within these year groups.
If parents have any queries or concerns in relation to online safety, these should be raised with the DSL or Online Safety Lead.

ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see Acceptable Use Policy). This also applies to the use of mobile phones and social media (see Mobile Phone Policy and Social Media Policy).

FILTERING OF DEVICES SYSTEMS IN SCHOOL

Our school use a filtering solution called Webscreen which is provided with our internet subscription to the London Grid for Learning. Webscreen is a flexible, safe web filter designed specifically for schools. The solution is based on an industry-leading web safety engine called Netsweeper. Webscreen constantly scans the school's internet traffic and categorises harmful materials. Webscreen prevents harmful material before it is displayed to the user in the form of a block screen warning. This enables the users to safely use the internet and provide logs for the designated safeguarding lead of what has been viewed, whose device and account information for monitoring purposes. In the event of harmful/inappropriate content being accessed, the block screen reminds users of the school's acceptable use policy and informs them that their search will be recorded. Webscreen streamlines a complex task to ensure that we are keeping children safe online in school.

MONITORING OF COMPUTERS IN SCHOOL

St Anselm's also use an eSafety solution called BeeSafe. This software is developed by Beebug and provides monitoring of all staff and student workstations whether on-site or off-site using cloud-based technology. BeeSafe constantly monitors users keyboard input as well as screen output to detect harmful keywords typed or seen on the screen this includes swearing, sexual content and words linked with extremism and/or terrorism. If harmful content is detected a screenshot (or capture) is taken with the user's computer name, IP address, username and timestamp. Captures are reviewed by eye and are collated ad-hoc by Beebug who send the schools designated safeguarding lead and computing technician a weekly or monthly report for review depending on what has been captured and when.

Filtering & monitoring Responsibilities:

The DSL is responsible for managing the filtering and monitoring systems in the school, working with the Online Safety lead and IT technician to ensure effective systems are in place.
If an online safety breach is identified through the filtering and monitoring systems, the IT technician must notify the Online Safety lead. This will then be dealt with accordingly and recorded on CPOMS in line with the behaviour policy. If an online safety breach is identified by a member of staff during a lesson, this must be recorded on CPOMS by the member of staff, which in turn notifies the DSLs.
An annual audit of the school's filtering and monitoring systems is conducted on an annual basis by the DSL, Online Safety lead and IT technician.
Half termly monitoring checks are conducted by two members of the online safety team to ensure that systems are working effectively. These are recorded centrally for audit purposes.
Filtering and monitoring breaches are promptly addressed by the DSL with the individual and parents, as well as through online safety teaching sequences.

RESPONDING TO ONLINE SAFETY CONCERNS

The safety of the child and young person is of paramount importance. Immediate action may be required to safeguard investigations and any other children and young people. Any concern that children and young people may be at risk of harm or abuse must immediately be reported. Reputational issues must be managed appropriately by discussion with the relevant communications team.

Online safety is recognised as part of the education settings safeguarding responsibilities – the DSL should take lead responsibility for online safety concerns which should be recorded and actioned. Children and young people will be enabled (at a level appropriate to their age and ability) to share online concerns. The child protection policy for St Anselm's includes procedures to follow regarding online safety concerns.

Remember:

- Child welfare is of principal concern – the best interests of children take precedence.
- If there is any immediate danger, contact the police on 999.
- Refer to all appropriate agencies as per St Anselm's local process- Harrow Children's Social Care and Multi-agency Safeguarding Hub (MASH).
- Report to the DSL.

Review

This policy will be reviewed annually, or earlier in the light of any incidents or investigations, legislative changes or developments in best employment practice, to ensure its continuing relevance and effectiveness.