St. Anne Line Catholic Junior School

E-Safety Policy

Reviewed: September 2024

ST. ANNE LINE CATHOLIC JUNIOR SCHOOL

E-Safety Policy

Wickhay,
Basildon
Essex.
SS15 5AF

Date of Policy:	September 2024
Date last review adopted by Governing Body:	September 2020
Date of next review:	September 2028

With Jesus, through the St Anne Line Way,
We Love, We Learn, We Share, We Pray.

Together, we grow Our School each day

1. Aims

Statement of Intent:

At St Anne Line Catholic Junior School, the safety of our pupils, staff, volunteers, and governors in the digital space is a priority. Our school recognises the evolving risks associated with technology use and online interactions. We are committed to implementing strong systems to ensure the online safety of everyone in our school community. This includes continuous education, proactive monitoring, and swift action when necessary to safeguard against potential harm.

Through a comprehensive and empowering approach, we aim to protect, educate, and foster responsible digital citizenship for our entire school community, including the responsible use of mobile and smart technology. In line with our values and ethos, we pledge to create a secure and supportive online environment where individuals are protected and supported in navigating the digital world safely.

Aims and Objectives of the Policy:

- To establish robust processes that ensure the online safety of pupils, staff, volunteers, and governors.
- To identify and support groups of pupils who are at a higher risk of online harm.
- To deliver an effective and empowering approach to online safety that educates the entire school community.
- To set up clear mechanisms for identifying, intervening, and escalating incidents where appropriate.

Statement of Principles:

- St Anne Line Catholic Junior School seeks to provide a safe and secure digital environment where all children and adults can learn, grow, and develop their digital skills without fear of harm.
- We are committed to fostering a culture of respect, understanding, and responsibility in the use of technology, ensuring that all individuals are treated fairly and without fear of intimidation.

- Our school will:
    - Actively listen to concerns related to online safety.
    - Respond appropriately to any incidents or information received to maintain a safe and secure online environment.
    - Ensure all pupils have the right to participate in their education without being subjected to harmful online content, interactions, or conduct.

The 4 Key Categories of Online Risk: Our approach to online safety addresses the following categories of risk:

- **Content:** Exposure to illegal, inappropriate, or harmful material such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
- **Contact:** Harmful interactions with others online, including peer pressure, commercial exploitation, and grooming or exploitation by adults posing as children or young adults for sexual, criminal, or financial purposes.
- **Conduct:** Personal behaviour online that increases the risk of harm, such as creating or sharing explicit images (e.g., nudes or pornography), or engaging in online bullying.
- **Commerce:** Risks related to online financial harm, such as gambling, phishing scams, inappropriate advertising, and other financial exploitation.

We are committed to maintaining and updating these practices to reflect the changing nature of online safety risks, ensuring our school community is protected, informed, and empowered.

2. 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
- 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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Steve Miles & the governor who oversees safeguarding is Roland Bremmer.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms set out in this policy.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL – Lisa Short) and deputies (Nathalie Watson & Nicole Sweeney) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL/DDSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged via CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board, including GDPR breaches
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- At St Anne Line Catholic Junior School, we conduct continuous security checks and monitoring of the school's ICT systems, ensuring ongoing protection at all times.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

3.5 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
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by logging it on CPOMs.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- 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

3.7 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.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools – as a Catholic School we follow the Journey in Love scheme of work.

Pupils in **Key Stage 2 (KS2)** will be taught to:

- 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) 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 about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

- The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website, newsletters updates or virtual learning environment (Teams). This policy will also be shared with parents/carers.
- Online safety will also be covered in an annual workshop offered to parents/carers.
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
- Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and social media policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

The Computing Lead, Nicole Sweeney, will conduct a whole-school assembly each term on online safety, supported by the Digital Leader team and the Anti-bullying Ambassadors.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected – sent out monthly attached to our school newsletter.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed.

7. Acceptable use of the internet in school

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school but are to leave them in the school office. They can then collect their device at the end of the school day.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software – this is completed by our ICT manager
- Keeping operating systems up to date by always installing the latest updates – this is completed by our ICT manager

If staff have any concerns over the security of their device, they must seek advice from the ICT manager (B.I.S) or Computing Lead (Nicole Sweeney).

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL [and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found electronically on CPOMs.

This policy will be reviewed every year by the Computing Lead and DDSL: Nicole Sweeney. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Social Media Policy
- Anti-bullying Ambassador Policy

Saint Anne Line Catholic Junior School is a level one Rights' Respecting school. At the heart of our school is the Convention for the Rights of the Child (CRC). This is evident in our planning, policies, practice and ethos.

- **Standard A: Rights-respecting values underpin leadership and management** The best interests of Saint Anne Line pupils are a top priority in all actions. The values and principles of the CRC at the heart of this policy.
- **Standard B: The whole school community learns about the CRC** The Convention is made known to children and adults. They use this shared understanding to work for global justice and sustainable living.
- **Standard C: The school has a rights-respecting ethos** Children and adults collaborate to develop and maintain a rights-respecting school community, based on the CRC, in all areas and in all aspects of school life.
- **Standard D: Children are empowered to become active citizens and learners** Every child has the right to say what they think in all matters affecting them and to have their views taken seriously. Saint Anne Line pupils develop the confidence, through their experience of an inclusive rights-respecting school community, to play an active role in their own learning and to speak and act for the rights of all to be respected locally and globally.