Sacred Heart R.C. Primary School

On-Line Safety Policy

Policy written by H. Rogerson Computing Leader Spring 2026

Accepted by Governors and Head teacher: *A. Herko* signed (Chair)

I. M Dermott signed (Head)

Shared with staff: Spring 2026

Shared with parents: Spring 2026

Mission Statement:

With Christ as our guide, we inspire and thrive.

As technology rapidly develops in today's worlds and becomes an essential part of society, we ensure our children learn how to access the digital world safely to communicate, play and learn. Online safety has a high profile at Sacred Heart RC Primary School for all stakeholders.

Our Online Safety curriculum is taught alongside our computing curriculum. We have designed our Computing Curriculum to teach an Online Safety unit at the start of each half term, with clear progression throughout each year group. This also weaves though all the lessons that we teach within Computing but also in RSE, PSHE and other curriculum areas. Our curriculum is supported through a nationwide programme called Project Evolve which teaches the children about online safety under these eight headings:

1. Self-image and identity

2. Online relationships

3. Online reputation

4. Online bullying

5. Managing online information

6. Health, wellbeing and lifestyle

7. Privacy and security

8. Ownership

These areas are explored by our children across all the age groups at a level that is suitable for them at the start of each half term. We also have specific safety moments through the year led by our computing lead and Digital Leaders. Furthermore, we participate in Safer Internet Day in the Spring term.

Aims

At Sacred Heart, we aim to have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors. Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones'.) Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi nudes and/or pornography), sharing other explicit images and online bullying.

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

We ensure the aims of this policy needs are met by the following:

- Ensuring that at the start of each half term we have an online safety lesson following the progression document.
- Highlighting issues relating to online safety as they link to the wider curriculum- especially in PSHE
- Training for staff and governors is relevant to their needs and ultimately positively impacts on the pupils.
- Pupils are prepared to be safe and responsible users online
- Through our home/school links and communication channels (especially the website and Facebook), parents are kept up to date with relevant online safety matters, policies, and agreements. They know who to contact at school if they have concerns.
- Pupils and staff have Acceptable Use Policies which outline the standards expected of users and procedures for non-compliance with the policy. (Signed by pupils at the beginning of each academic year.)
- Data policies stipulate how we keep confidential information secure in line with GDPR.
- Staff have access to the National Online Safety website and can direct parents to appropriate materials from there as needed.
- Using Digital Leaders to disseminate online safety information to the school community.

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping children safe in education2, and its advice for schools on:

- teaching online safety in schools
- preventing and tackling bullying : Preventing bullying - GOV.UK- advice for head teachers and staff
- Relationships and sex education (RSE) and Health Education
- Searching, screening and confiscation

The policy also refers to the DfE's guidance on protecting children from radicalisation. The policy reflects existing legislation, including but not limited to the Education Act 1996 (as amended), Education and Inspections Act 2006 and Equality Act 2010 . In addition, the policy reflects Education Act 2011 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.

Roles and responsibility

All members of the school community have a duty to be aware of online safety at all times and to know the required procedures and to act on them. The following responsibilities demonstrate how each member of the community will contribute.

The Governing Board is responsible for ensuring the effectiveness of the policy and holding the headteacher to account for its implementation. The Governing Board are responsible for being aware of the current issues in online safety, reviewing (anonymised) incidents and filtering and monitoring logs (CPOMS) as provided by the designated safeguarding lead (DSL.) The Safeguarding Governor will monitor this area and regularly meet with DSL. All governors will ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

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

Safeguarding Lead (DSL) is responsible for: being aware of the potential for serious safeguarding issues to arise from: sharing of personal data, access to illegal/inappropriate materials, and inappropriate online contact with adults/strangers, potential or actual incidents of grooming, online bullying. Taking day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns. Working alongside computing lead, they will promote an awareness of, and commitment to, online safety both in school and out. They will also 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. Furthermore, they are responsible for liaising with other agencies and/or external services if necessary

Staff are responsible for reading, understanding and implementing this policy. They will monitor what is on pupils' screens and teach pupils about online safety. They are responsible for ensuring all online safety incidents, including sexual violence/harassment and cyber bullying, are dealt with appropriately in line with our behaviour policy and antibullying policy and are logged on CPOMS. Staff will also main a professional level of conduct in the personal use of technology and model safe and responsible behaviours in their own usage.

Technical Staff, abtec, are responsible for reading, understanding and contributing to this policy. They will provide and take responsibility for a safe and secure technical infrastructure to support learning and teaching by ensuring that appropriate physical access controls exist to control access to information systems, networks and telecommunications equipment situated within school. It is their responsibility to ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. They will maintain an awareness of current online safety issues, legislation and guidance relevant to their work and pass any such information to the headteacher. Abtec staff will ensure that provision exists for misuse detection and malicious attack and document all technical procedures and review them for accuracy at appropriate intervals.

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.

Parents are responsible for helping and supporting the school in promoting online safety and consulting with the school if they have any concerns about their children's use of technology

Parents/carers can seek further guidance on keeping children safe online by clicking on the **Thinkuknow** links on school's website Computing - Sacred Heart Atherton or from the following organisations and websites:

• What are the issues? – What are the issues? - UK Safer Internet Centre

• Hot topics – Help & advice | Childnet

• Parent resource sheet – Parents and Carers resource sheet | Childnet

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

Teaching and Learning

At Sacred Heart, we believe that the key to developing safe and responsible behaviours online, not only for children but for everyone within our school community, lies in effective education. We understand that the internet and other technologies in our children's lives both in school and out, is our duty to prepare them to be safe online. Children will be taught about online safety as part of the curriculum, but not limited to computing.

In Key Stage 1, children will be taught to:

- 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.

In Key Stage 2, children 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, children 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, for example within the schools PSHE and RSE curriculum.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

<u>Learning</u>

We take online safety very seriously and we aim to give children the necessary skills to keep themselves safe online. Children have a right to enjoy childhood online, to access safe online spaces and to benefit from all the opportunities that a connected world can bring them, appropriate to their age and stage.

- Pupils will be taught that some internet use is responsible and that some is not and will be given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation -appropriate to their age group.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Online safety will also be discussed where appropriate in all lessons where the use of digital technologies are incorporated.
- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology. They

will be taught to tell an adult about malicious or harmful content they may encounter from their peers in line with guidance in KCSIE 2025

- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location.
- Lessons will be used to educate pupils about cyber bullying, including how to report cyber-bullying.
- Children will be taught how to protect themselves against the risks of being groomed online for exploitation or radicalisation in line with the guidance outlined in the Prevent strategy.
- Children will be taught about the risks of accessing and generating inappropriate content.

Acceptable use of the internet

All pupils, parents, staff, volunteers and governors are expected to sign accept an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. 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. Securus (Senso) monitoring and filtering system is installed and this is regularly by the headteacher.

Filtering and Monitoring

At Sacred Heart, we use a filtered internet service provided by abtec. The provision includes filtering appropriate to the age and maturity of pupils and we are proactive regarding the nature of content which can be viewed.

- In the first instance children are kept safe by being directed to use appropriate online resources. 'Shoulder surfing' by the teacher ensures that the children are accessing the correct material.
- All pupils are provided with a username and password so that content can be monitored on a regular basis. Online activity can be tracked. Individual log ins for Purple Mash mean teachers can remotely check pupils' work and log in times.
- Webpages are filtered to prevent inappropriate use of the internet. At Sacred Heart we use a piece of software called Securus to help protect our children. Securus is a leading online safety solution, protecting students and staff by alerting safeguarding teams to inappropriate or potentially harmful behaviour. Senso helps us to comply with KCSIE 2025 and the Prevent Duty guidance.

Communications

Any mobile phones or gaming tablets should not be brought onto the school premises by pupils unless specifically instructed by the class teacher. Apart from Y6 (and other known pupils where appropriate) where their phones may be kept in the school office.
Any communication via social media should be done so through the school's official accounts. Teachers and teaching assistants should not be contacted through their personal social media accounts and staff should not accept friend requests from parents or pupils (present and former).

Use of digital and video images

- Children should be educated by staff and parents on the risks of sharing images and information online.
- Staff are allowed to photograph children in school for educational uses. Parents must give consent for pupils' images to be shared on the school website and via social media.
- When permission is given parents and carers are welcome to take photographs of their children during school events but we ask that these are not shared online.

Managing failures in online safety

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 or tablet. School will deal with failures in online safety in the following way:

- Teacher's will minimise the immediate risk to children by completing a dynamic risk assessment and acting accordingly- this might mean stopping access for one pupil or it might mean immediately stopping access for a whole class.
- Computing Leader and SLT to be informed (via email).
- If a user discovers a website with inappropriate or potentially illegal content, these are to be immediately reported to class teacher.
- Inappropriate access to be investigated by Computing Leader to check whether it was intentional or unintentional. If intentional then sanctions to be put in place in line with AUP and behaviour policy and antibullying policy.
- Any inappropriate access whether intentional or unintentional will be reported to parents.
- The school will immediately audit filtering and monitoring provision to establish if it is adequate and that its implementation is effective.

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. Not sharing the device among family or friends Installing anti-virus and anti-spyware software Keeping operating systems up to date – always install the latest updates.

This policy will be reviewed regularly in consultation with staff and following any national initiatives. A copy will be available on the school website.

Reviewed: Spring 2026

Next review: Spring 2027