Sacred Heart Catholic Primary School

Online Safety Policy

Dated: February 2024

To be reviewed: 2026

Signed…….Headteacher

Signed…….Chair of Governors

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, and Relationships and sex education.

It also refers to the DfE's guidance on protecting children from radicalisation (PREVENT) It reflects existing legislation, including but not limited to the Education Act 1996, 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 and the acceptable use policies for staff, pupils and families. This policy also complies with our funding agreement and articles of association.

Intent

It is the intent of all staff and leaders at Sacred Heart School to:

-Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors

-Identify and support groups of pupils that are potentially at greater risk of harm online than others –

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 - To educate and protect pupils from the 4 key categories of risk:

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

Contact – being subjected to harmful online interaction with other users, such as child on child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, sharing other explicit images and online bullying; and

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

-To build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. -To demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks.

The Role of the Governing Body

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, 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. They 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 those 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 Mr. Michael Payne

All governors will:

Ensure they have read and understand this policy

• Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

• Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

• 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.

The role of the headteacher

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

The role of the designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL and Deputies take lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the 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 Computing Lead and ICT technician to make sure the appropriate systems and processes are in place e.g. SENSO and RM

- Working with the headteacher, Computer Lead 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 on 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 - 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

The role of ICT technician

-Liaising with DSL to put 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

- Conducting a full security check and monitoring the school's ICT systems on a monthly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The role of Computing and Online Safety Lead

- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Meet with link governor to review monitoring termly.
- Ensure staff confidence in teaching online safety is high through effective and regular training and support
- Ensure parents and carers feel supported and informed on the risks posed by online use through documentation, workshop opportunities and website communication

The school has an appointed Online safety Lead– Mrs Hazel Ellmore

The role of 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
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- 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 speaking to the DSL, reporting on CPOMS or making a 'low-level' concern referral.
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes.

- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- 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'

The role of Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Check the Holy Rood school website regularly for updates on keeping their child safe online and to find ways to make a referral if you are concerned that a child may be at risk (CEOP)
- 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 International
  - Parent resource sheet – Childnet International

The role of 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.

Email & Online Collaboration

- Pupils may only use approved school email accounts on Microsoft Teams
- Email accounts have been created for each child at Sacred Heart School with enhanced safeguarding measure in place to ensure our pupils safety as much as possible.
- Pupils must immediately tell a teacher if they receive offensive messages.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Pupils may must not access others pupil's accounts or files
- Pupils must be responsible for their own behaviour on the Internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Pupils must not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site.

- Pupils are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.
- Pupils must ask permission before accessing the Internet and have a clear idea of why they are using it.
- Computers and school laptops should only be used for schoolwork and homework unless permission has been given otherwise.
- No program files may be downloaded from the Internet to the computer, to prevent corruption of data and to avoid viruses.
- Pupils must not bring in USBs from home for use in school without permission. This is for both legal and security reason. USBs should be virus scanned before use.
- Access in school to external personal email accounts may be blocked.
- Pupils must sign an agreement form if using school device at home which includes a code of conduct

Social Networking

At Sacred Heart School we block/filter access to social networking sites and newsgroups unless a specific use is approved

- Pupils are advised never to give out personal details of any kind, which may identify them or their location
- Pupils are advised not to place personal photos on any social network space
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are encouraged to invite known friends only and deny access to others
- Pupils and parents are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube or Instagram is 13 years old.

Filtering

The school will work in partnership with our Internet Service Provider to ensure filtering systems are as effective as possible. The DSLs will monitor the school's filtering systems outside of managing instant alerts to ensure pupil safety online remains our priority.

RM Safety Net Aligned with the DfE's definition of appropriate filtering within the Keeping Children Safe in Education (KCSiE), RM SafetyNet will;

• Carry out user-based reporting

• Monitor school-wide internet activity

• Switch on appropriate filtering for the age groups of pupils in our school All Illegal websites are blocked by RM SafetyNet based on input from the Internet Watch Foundation, the Home Office, the Counter Terrorist list and security intelligence, including radicalisation content. Our technology safeguards devices brought into school when they're connected to the network.

RM Safety Net

Aligned with the DfE's definition of appropriate filtering within the Keeping Children Safe in Education (KCSiE), RM SafetyNet will:

• Monitor school-wide internet activity

• Switch on appropriate filtering for the age groups of pupils in our school

All Illegal websites are blocked by RM SafetyNet based on input from the Internet Watch Foundation, the Home Office, the Counter Terrorist list and security intelligence, including radicalisation content. Our technology safeguards devices brought into school when they're connected to the network.

SENSO

SENSO provides a top-level overview for DSLs by reporting all violations across school devices. Senso's internet monitoring and pupil safety software is designed to enhance pupil safety with live alerts, keyword monitoring, website logs and blocks which are reported instantly to DSLs in school for action to be taken. This will then be logged onto CPOMs via the 'Online Safety-tag.

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.

In Key Stage 1, pupils 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.

Pupils in Key Stage 2 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.

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. This policy will also be shared with parents/carers online.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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.

Cyber-bullying

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 the school behaviour policy.)

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. We will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (RSHE/PSE) education, and other subjects where appropriate.

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.

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

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher (DSL).
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to Headteacher and DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image

- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with: The DfE's latest guidance on searching, screening and confiscation UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to read to demonstrate an agreement of 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 and restrict access through filtering systems where appropriate.

Pupils using mobile devices in school

Pupils in year 6 only may bring mobile devices into school if they are walking to or from school alone and therefore need them for communication with a parent/carer. The mobile phone must be switched off between 8:45am and 3:15pm and only used before or after to contact a parent/carer. The phone MUST be handed to the class teacher or school office. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure and are used in line with the school's staff acceptable use policy. This includes:

- 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 sensitive content 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
- Keeping operating systems up to date by always installing the latest updates
- Staff members must not use the device in any way that would violate the school's terms of acceptable use e.g. using messaging apps, social media pages or viewing/using inappropriate words or content
- Work devices must be used solely for work activities. - If staff have any concerns over the security of their device, they must seek advice from the ICT technician or DSL.

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 policy]. 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, staff code of conduct and 'low level' concerns report. 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.

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 staff handbook, emails, bulletins 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, 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS. All Staff will also report concerns vis CPOMs which the Headteacher/DSL will always view and action. This policy will be reviewed every year by the Online Safety Lead. At every review, the policy will be shared with the governing board.

Links with other policies This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Code of Conduct for Staff
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy