HOLY FAMILY CATHOLIC SCHOOL

ONLINE SAFETY POLICY

Date agreed	October 2025
Next review date	October 2026

Holy Family Catholic School Online Safety Policy
In line with Keeping Children Safe in Education 2025

---

1. Introduction and Context

Holy Family Catholic School recognises that it is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. Keeping Children Safe in Education
This policy acknowledges that abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults or by another child or children. Keeping Children Safe in Education
This policy should be read in conjunction with our Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and Mobile Phone Policy.

2. Policy Statement and Aims

This policy aims to:

- Set out expectations for all members of the school community regarding safe and responsible use of technology
- Establish clear mechanisms to identify, intervene in, and escalate concerns where appropriate
- Safeguard and protect all members of our school community online
- Identify approaches to educate and raise awareness about online safety throughout the school community
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns

3. Roles and Responsibilities

3.1 The Governing Body

The governing body is responsible for making sure filtering and monitoring is in place. The board should review the DfE's filtering and monitoring standards and discuss with IT staff and service providers how they can support the school to meet those standards. The governing body should assign a governor or member of staff to make sure these responsibilities are being met and identify and assign the roles and responsibilities of staff and third parties. The Key Leaders Keeping Children Safe in Education
The governing body is responsible for making sure that the effectiveness of filtering and monitoring measures is reviewed at least annually and after any significant equipment or system changes. The Key Leaders

3.2 The Headteacher

The Headteacher has overall responsibility for online safety and for ensuring this policy is implemented and its effectiveness reviewed.

3.3 The Designated Safeguarding Lead (DSL)

The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). Keeping Children Safe in Education

The DSL needs to take lead responsibility for online safety including filtering and monitoring systems and processes, understand the risks associated with online safety, be confident that they have the relevant knowledge and up-to-date capability required to keep pupils safe while they are online at school, and recognise the additional risks that pupils with SEND face online, including from bullying, grooming and radicalisation.

3.4 All Staff

All staff should undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. In addition, all staff should receive regular safeguarding and child protection updates, including online safety (for example, via email, e-bulletins, staff meetings) as required, and at least annually. Keeping Children Safe in Education
All staff should carry out in-person monitoring in rooms with pupils using devices as part of wider classroom observation. The Key Leaders

4. The 4Cs: Understanding Online Safety Risks

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories
- **Contact**: being subjected to harmful online interaction with other users; for example: 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**: online behaviour that increases the likelihood of, or causes, harm; for example, 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 scams Keeping Children Safe in Education

5. Education and Curriculum

5.1 Teaching Pupils About Online Safety

Children are taught about how to keep themselves and others safe, including online. Effective education is tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs and/or disabilities (SEND).

In schools, relevant topics are included within Relationships Education (for all primary pupils), and Relationships and Sex Education (for all secondary pupils) and Health Education (for all primary and secondary pupils).

At Holy Family Catholic School, our online safety education programme tackles, at an age-appropriate stage, issues such as:

- Supporting children to develop the skills that form the building blocks of all positive relationships
- Healthy and respectful relationships

- Boundaries, consent and kindness in relationships
- Stereotyping, prejudice and equality
- Body confidence and self-esteem
- How to recognise and report concerns about an abusive relationship, including coercive and controlling behaviour
- The concepts of, and laws relating to all forms of sexual harassment, and abuse, and how to access support
- What constitutes sexual harassment and sexual violence and why these are always unacceptable, emphasising that it is never the fault of the person experiencing it

5.2 Staff Training

Safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning. Keeping Children Safe in Education

6. Child-on-Child Abuse

All staff should be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school and online.

Child-on-child abuse is most likely to include, but may not be limited to:

- Bullying (including cyberbullying, prejudice-based and discriminatory bullying)
- Abuse in intimate personal relationships between children (sometimes known as 'teenage relationship abuse')
- Physical abuse (this may include an online element which facilitates, threatens and/or encourages physical abuse)
- Sexual violence and sexual harassment (including online sexual harassment, which may be standalone or part of a wider pattern)
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
- Upskirting
- Initiation/hazing type violence and rituals (which may also include an online element) Keeping Children Safe in Education

7. Mobile and Smart Technology

The school has a clear policy on the use of mobile and smart technology, which reflects the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Keeping Children Safe in Education
[School to insert specific mobile phone policy provisions here]

8. Filtering and Monitoring

8.1 Systems and Standards

The Department for Education's filtering and monitoring standards set out that schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually

- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs
- Schools can use the department's 'plan technology for your school service' to self-assess against the filtering and monitoring standards and receive personalised recommendations on how to meet them

8.2 Appropriate Filtering

As a starting point, the school will:

- Enable safe search on any search engines used (or use a child-friendly search engine)
- Make sure that any devices brought into the school have adequate filtering and monitoring measures in place
- Be aware of new technologies that might impact filtering and monitoring (e.g. generative AI, virtual private networks or proxy networks) The Key Leaders

The school's filtering systems have separate profiles for staff and pupils to allow different levels of access to the internet.

8.3 Avoiding Over-Blocking

Whilst it is essential that appropriate filtering and monitoring systems are in place, the school is careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

9. Cyber Security

The school is directly responsible for ensuring it has the appropriate level of security protection procedures in place in order to safeguard its systems, staff and learners and reviews the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The school considers taking appropriate action to meet the Cyber security standards for schools and colleges which were developed to help improve resilience against cyber-attacks.

10. Remote Learning and Safeguarding

When pupils are learning online from home, the school has appropriate safeguarding measures to keep teachers and pupils safe. When communicating with parents and carers, the school reinforces the importance of online safety, including making parents/carers aware of what pupils are asked to do online (e.g. sites they need to visit or who they'll be interacting with online).

11. Responding to Online Safety Incidents

11.1 All Staff

If staff have any concerns about a child's welfare, they should act on them immediately. They should follow the school's child protection policy and speak to the designated safeguarding lead (or a deputy). In the absence of the designated safeguarding lead (or a deputy) staff should speak to a member of the school's senior leadership team.
The designated safeguarding lead (or a deputy) will generally lead on next steps, including who else, if anyone, in the school should be informed and whether to pass a concern to local authority children's social care and/or the police. Keeping Children Safe in Education

11.2 Specific Online Safety Concerns

The school will respond to specific online safety concerns including:

- **Cyberbullying**: Following our anti-bullying policy and behaviour policy
- **Sharing of nudes and semi-nudes**: Following UKCIS guidance "Sharing nudes and semi-nudes: advice for education settings working with children and young people"
- **Online sexual harassment**: Following Part 5 of KCSIE 2025
- **Cybercrime**: Considering referral to the Cyber Choices programme where appropriate
- **Radicalisation online**: Following the Prevent duty and making referrals to Channel where appropriate

12. Working with Parents and Carers

Involving parents and carers with online safety allows staff, and parents/carers to work together. Parents/carers can:

- Share any online safety issues that occur at home, to help the school design online safety programmes that reflect these issues
- Implement the same principles of online safety at home
- Gain a better awareness of the school's curriculum The Key Leaders

The school will:

- Communicate with parents/carers about online safety through newsletters, the school website, and parent workshops
- Provide parents/carers with information about filtering and monitoring systems
- Share factsheets about popular apps, games and websites
- Direct parents/carers to useful resources such as those from the NSPCC, Internet Matters, Childnet, and CEOP

13. Monitoring and Review

The school carries out an annual review of its approach to online safety, supported by an annual risk assessment that considers and reflects the risks pupils face.

This policy will be reviewed annually by the governing body in consultation with the Headteacher and Designated Safeguarding Lead.

14. Related Policies and Guidance

This policy should be read in conjunction with:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Acceptable Use Policy (Staff and Pupils)
- Data Protection Policy
- Relationships and Sex Education Policy

15. Useful Resources and Links

- UK Safer Internet Centre: https://saferinternet.org.uk/
- NSPCC Online Safety: https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- Childnet: https://www.childnet.com/
- Internet Matters: https://www.internetmatters.org/

- CEOP Education: https://www.thinkuknow.co.uk/
- National Cyber Security Centre: https://www.ncsc.gov.uk/