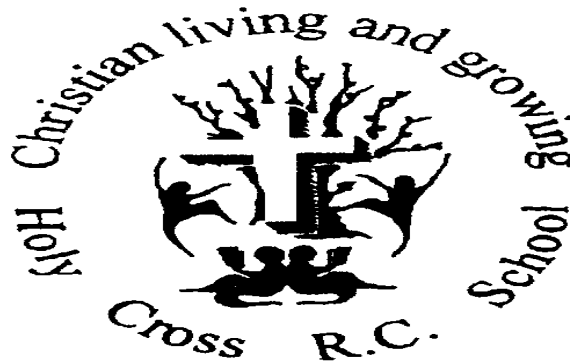


Holy Cross RC Primary School



Online Safety Policy

Signed _____ [Headteacher] Date _____

Signed _____ [Chair of Governors] Date _____

Review Date November 2025

Next Review Date

November 2026

Contents:

- 1) Aims
- 2) Legislation and guidance
- 3) Role and responsibilities
- 4) Educating pupils about online safety
- 5) Examining electronic device
- 6) How the school will respond to issues of misuse
- 7) Monitoring
- 8) Remote learning
- 9) Training

1) Aims

Holy Cross Catholic Primary School aims 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2) Legislation and guidance

This policy is based on the Department for Education's (DfE) 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](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- It also refers to the Department'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 program of study.

3) Roles and responsibilities

All staff at Holy Cross are responsible for the implementation of this policy.

Within our school the Headteacher, Designated Safeguarding Leads (DSL) and Online Safety coordinator are responsible for ensuring this policy is implemented and consistent throughout the school.

- The Online Safety Coordinator 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
 - Ensuring that any online safety incidents are logged 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

Alongside the Head Teacher, DSL and Online Coordinator, our Business manager also liaises with our IT services, support with:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged 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

4) Educating pupils about online safety

Intent:

At Holy Cross we aim to provide our pupils with the knowledge, skills and understanding to safely navigate the online world both inside and outside of school. We provide the children with an Online Safety curriculum that is purposeful and provides children with this knowledge.

Implementation:

Pupils will be taught about Online Safety as part of the curriculum from the National Curriculum Computing Programmes of study we are using Project Evolve to help support the delivery of these objectives. Alongside the standalone lessons we also cover Online Safety through PSHE (Scarf) and regularly throughout the school year on such events as Safety Week and Safer Internet Day. We provide the children with safe spaces and age appropriate resources to highlight key skills in the following areas: Self image and Identity, Online Relationships, Online Reputation, Online Bullying, Privacy and Security and Health and Wellbeing online. In all Computing lessons the online safety rules will be discussed and reiterated to the children. Children will also take part in Computing events throughout the year such as: Safer Internet Day, NSPCC workshops/ assemblies and Anti-Bullying week.

Impact:

Through the use of the Online Safety curriculum and policy all staff have access to the relevant information and technical skills to deliver lessons to the

children. Staff will be equipped with the most up to date knowledge thus ensuring our children are competent, caring and safe users of the digital world. Children will see the digital world as part of their world, extending beyond school, and understand that they have choices to make. They will be confident and respectful digital citizens going on to lead happy and healthy digital lives.

In EYFS, pupils will be taught to:

Personal, Social and Emotional Development

- Show resilience and perseverance in the face of a challenge.
- Know and talk about the different factors that support their overall health and wellbeing: -sensible amounts of 'screen time'.

Physical Development

- Develop their small motor skills so that they can use a range of tools competently, safely and confidently.

Expressive Arts and Design

- Explore, use and refine a variety of artistic effects to express their ideas and feelings.

Early Learning Goals:

Personal, Social and Emotional Development Managing Self

- Be confident to try new activities and show independence, resilience and perseverance in the face of challenge.
- Explain the reasons for rules, know right from wrong and try to behave accordingly.

Expressive Arts and Design Creating with Materials

- Safely use and explore a variety of materials, tools and techniques, experimenting with colour, design, texture, form and function.

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
 - How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Education – Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of children in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and cross curricular activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices. For example: all Youtube videos/ media should be previewed in advance of the session to ensure it is appropriate and the ensure there are no adverts which may be inappropriate.
- in lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, Class Dojo, Social media pages and Tapestry pages
- Parents / Carers evenings / sessions, at the beginning of assemblies
- High profile events / campaigns eg Safer Internet Day

5) Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6) 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 and Online Safety 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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

7) Monitoring arrangements

The DSL and Online Safety lead log behaviour and safeguarding issues related to online safety. These will be recorded on CPOMS and using the Online Safety incident log.

8) Remote Learning

In March 2020 To help protect communities from coronavirus (COVID-19), schools and educational settings were closed, except to the children of critical workers and vulnerable children and the staff needed to look after them. In that time education moved to online platforms. Our school used G-Suite for education (Google Classroom), Class Dojo and Tapestry to set work and keep in communication with the cohort.

To support online learning during lockdown there were dedicated sessions for online safety fortnightly using Thinkuknow resources (<https://www.thinkuknow.co.uk/parents/support-tools/home-activity-worksheets/>).

During this time, a Remote Learning Policy was created, please see for further information.

As of September 2021, the need for remote learning has been reduced however all staff must ensure they are able to offer high quality remote learning, access the school lessons and resources if the need arises. We will again achieve this through Google Meet and Google Classroom. All teachers now have webcams in their classrooms to help facilitate this process.

9) 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, e-bulletins and staff meetings).

The DSL [and deputy/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.