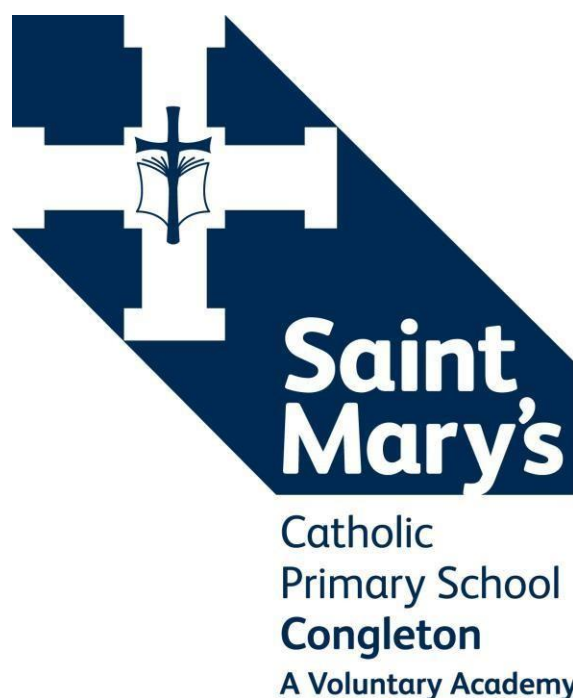


Saint Mary's Catholic Primary



Online Safety Policy

Policy Schedule	Date	Signed
Approved by the Governing Body:	May 2026	Headteacher: Amy Butterfield Chair of Governors: Val Bridge
To be Reviewed	May 2028	

1. Catholic Ethos and Aims

As a Catholic primary school, our approach to online safety is deeply rooted in our Gospel values. We believe in the dignity of every human person, and we teach our pupils that the respect and kindness they show others in the physical world must seamlessly extend into the digital world.

Our 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 (KCSIE), and reflects the latest statutory requirements regarding filtering and monitoring on school devices.

It also relies on DfE 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.
- Protecting children from radicalisation.

It reflects existing legislation, including the Education Act 1996, the Education and Inspections Act 2006, the Equality Act 2010, and the Education Act 2011, which gives teachers powers to tackle cyber-bullying by searching for and deleting inappropriate files on pupils' electronic devices if there is a 'good reason' to do so. It also complies with the National Curriculum computing programmes of study, our funding agreement, and articles of association.

3. Roles and Responsibilities

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 co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs.
- The governor who oversees online safety is Paul Fagan.
- Governors will ensure that online safety is a running and interrelated theme in the whole-school approach to safeguarding.
- Governors are responsible for ensuring the school meets the DfE's filtering and monitoring standards.

The Headteacher

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

The Designated Safeguarding Lead (DSL)

- The DSL takes lead responsibility for online safety in school.
- The DSL will work with the headteacher, ICT manager, and staff to address online safety issues.
- They will ensure online safety incidents are logged on CPOMS and dealt with appropriately.
- The DSL is responsible for updating and delivering staff training on online safety.
- The DSL holds primary operational responsibility for monitoring filtering and monitoring reports, taking action on safeguarding alerts.

The ICT Manager

- Responsible for putting in place appropriate filtering and monitoring systems to keep pupils safe from potentially harmful content and contact, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure, protected against viruses/malware, and updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and preventing the downloading of potentially dangerous files.

All Staff and Volunteers

- Implementing this policy consistently and maintaining an understanding of it.
- Agreeing to the acceptable use of the school's ICT systems and ensuring pupils follow the school's terms.
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately.
- Staff must understand their role in checking that filtering and monitoring systems are active and report any bypasses or failures immediately.

Parents

- Parents are expected to ensure their child has read, understood, and agreed to the acceptable use of the school's ICT systems.
- Parents should notify a member of staff or the headteacher of any concerns or queries regarding this policy.

4. Educating Pupils About Online Safety

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

- **In Key Stage 1**, pupils will be taught to use technology safely and respectfully, keeping personal information private, and identifying where to go for help.
- **In Key Stage 2**, pupils will be taught to use technology responsibly, recognise acceptable/unacceptable behaviour, and identify a range of ways to report concerns.
- By the end of primary school, pupils will understand that people sometimes behave differently online and that face-to-face relationship principles (including respect and dignity) apply online.
- They will learn how to recognise risks, critically consider their online friendships, understand how data is shared, and respond safely to unknown adults online.

5. Educating Parents About Online Safety

- The school will raise parents' awareness of internet safety via letters, the school website, weekly newsletters, and Google Classroom.
- Webinars, training, and guidance can be accessed via the National Online Safety app/website (<https://nationalonlinesafety.com/>).
- Online safety will be covered during parents' evenings.
- The school will let parents know what systems are used to filter and monitor online use, and what their children are being asked to do online.

6. Cyber-Bullying

- **Definition:** Cyber-bullying takes place online (e.g., social networking, gaming sites) and is the repetitive, intentional harming of one person or group by another, involving an imbalance of power.
- **Prevention:** The school will actively discuss cyber-bullying with pupils, exploring reasons it occurs and its consequences. Teaching staff will use PSHE and other subjects to cover cyber-bullying.
- **Response:** If 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 consider police involvement if illegal material is present.

7. Examining Electronic Devices

- School staff have the specific power under the Education and Inspections Act 2006 (increased by the Education Act 2011) to search for and delete inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
- Only the headteacher and authorised members of staff can search for and confiscate electronic devices, and must have reasonable grounds for suspecting the device poses a risk.
- If staff suspect a device contains a nude or semi-nude image, or an image that is a criminal offence to possess, they will **not view the image** but will immediately report this to the DSL.

8. Acceptable Use of the Internet in School

- All pupils, parents, staff, volunteers, and governors must sign an agreement regarding acceptable use.
- Use of the school's internet must be for educational purposes only or for fulfilling role duties.
- The school will monitor websites visited by all users to ensure compliance.
- Artificial Intelligence (AI): Staff and pupils must use generative AI tools responsibly. AI should not be used to bypass learning or assessments, and personal/sensitive data must never be inputted into public AI platforms. Our chosen AI platform is Co-Pilot inline with OLHOC.

9. Mobile Devices in School

- Pupils may bring mobile devices into school, but are not permitted to use them during lessons, before/after school clubs, or any other school-organised activities.
- Pupils should drop off their mobile phones at the school office at the start of the day and collect them at the end of the day.
- Breaching the acceptable use agreement may trigger disciplinary action, which may result in device confiscation.

10. Staff Using Work Devices Outside School

All staff must take appropriate steps to keep devices secure:

- Keep the device password-protected (at least 8 characters, with upper/lower-case letters, numbers, and special characters).
- Ensure the hard drive is encrypted.
- Ensure the device locks if inactive.
- Do not share the device with family or friends.
- Install anti-virus and anti-spyware software, and keep operating systems up to date.
- Work devices must be used solely for work activities.

11. Responding to Misuse

- Pupil misuse will follow procedures in the behaviour policy; action will be proportionate to the incident.
- Staff misuse will be dealt with in accordance with the Trust Personnel Handbook.
- The school will consider reporting serious incidents or illegal activity to the police.

12. Training

- All new staff receive induction training on safe internet use, cyber-bullying, and the risks of online radicalisation.
- All staff receive refresher training at least once each academic year.
- The DSL and deputy will undertake child protection and safeguarding training (including online safety) at least every 2 years, and update their knowledge at least annually.
- Governors will receive training on safe internet use and online safeguarding.

13. Monitoring and Links

- The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.
- This policy links to our Child Protection and Safeguarding Policy, Behaviour Policy, Staff Disciplinary Procedures, Data Protection Policy, Complaints Procedure, and ICT Acceptable Use Policy.

