Online Safety Policy

St Mary's Catholic Primary School

Version 1.0

Last Reviewed	**June 2026**
Reviewed By (Name)	**Alex Downing**
Job Role	**Deputy Head Teacher**
Next Review Date	**April 2027**
Version produced Spring 2026	

This document will be reviewed annually and sooner when significant changes are made to the law.

Guidance from the Department for Education about St Mary's Catholic Primary School policies can be found here: https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts

This policy is a direct response to the Keeping children safe in education (KCSIE) statutory guidelines.

Education Data Hub would like to give thanks and acknowledge SWGfL whose policies, documents and guidance have contributed to the development of this Online Safety Policy template. Their excellent resources that can help with this policy can be found here: Free Online Safety Policy Templates for Schools | SWGfL

Contents

1. Introduction

The school's approach to online safety is based on addressing the following categories of risk as set out by the Keeping children safe in education (KCSIE) statutory guidelines:

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 nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard pupils in the digital world
- describes how the school will help prepare pupils to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related policies: Behaviour; Child Protection & Safeguarding; Relationships, Sex & Health Education
- is made available to staff at induction and through normal communication channels
- is published on the school website

2. Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of St Mary's Catholic Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

St Mary's Catholic Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place outside of the school.

3. Roles and Responsibilities

Online safety is a team effort, so the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

3.1. Headteacher and Senior Leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those within the school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

3.2. Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by the pastoral committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of online safety governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant governors meeting

- Receiving cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

3.3. Designated Safeguarding Lead (DSL)

The DSL will:

- lead on online safety.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings
- report regularly to the headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- 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
- provide (or identify sources of) training and advice for staff/governors/trustees/parents/carers/pupils
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)

- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

3.5. Curriculum Leads

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- A discrete programme
- PSHE and RHE programmes
- Cross-curricular links
- Assemblies and pastoral programmes
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week

3.6. Teaching and Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with pupils, parents and carers and others should be on a professional level and only carried out using authorised school systems and devices (where staff use AI, they should only use authorised AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements)
- they immediately report any suspected misuse or problem to a DSL for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure pupils understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices

- in lessons where internet use is pre-planned pupils are 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

- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies

- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc

- they model safe, responsible, and professional online behaviours in their own use of technology, including outside of the school and in their use of social media.

- they adhere to the school's IT Acceptable Use policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity

- they have a general understanding of how the pupils in their care use digital technologies outside of the school, in order to be aware of online safety issues that may develop from the use of those technologies

- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in the school and the AI policy

3.7. IT Provider

If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and IT Acceptable Use Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored so that that any misuse/attempted misuse can be reported to DSLs for investigation and action

- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly updated as agreed in school policies

3.8. Pupils

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- should understand the importance of adopting good online safety practice when using digital technologies outside of the school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

3.9. Parents and Carers

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- Regular opportunities for engagement with parents/carers on online safety issues
- High profile events / campaigns e.g. Safer Internet Day
- providing them with a copy of the pupil acceptable use agreement acknowledged by signatures
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to pupils in the school
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

3.10. Community Users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to agree to an acceptable use agreement before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools/trusts/academies and the community.

4. Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and the governing body.

The Online Safety Group has the following members:

- Designated Safeguarding Lead
- online safety governor
- technical staff
- teacher and support staff members
- pupils
- parents/carers

Members of the Online Safety Group will assist the DSL with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of pupils to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions.

5. Acceptable Use

The Online Safety Policy, IT Acceptable Use Policy and acceptable use agreements define acceptable use at the school. These will be communicated/re-enforced through:

- Pupil planner

- Staff planner
- Splash screens
- Digital signage
- Posters/notices around where technology is used
- Communication with parents/carers
- Built into education sessions
- School website
- Peer support

6. Reporting and Responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.

- All members of the school community will be made aware of the need to report online safety issues/incidents.

- Reports will be dealt with as soon as is practically possible once they are received.

- The Designated Safeguarding Lead, and other responsible staff have appropriate skills and training to deal with online safety risks.

- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures, this may include:
  - Non-consensual images
  - Self-generated images
  - Terrorism/extremism
  - Hate crime/ Abuse
  - Fraud and extortion
  - Harassment/stalking
  - Child Sexual Abuse Material (CSAM)
  - Child Sexual Exploitation Grooming
  - Extreme Pornography
  - Sale of illegal materials/substances
  - Cyber or hacking offences under the Computer Misuse Act
  - Copyright theft or piracy

- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT.

- Where there is no suspected illegal activity, devices may be checked using the following procedures:

- One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.

- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by local authority
  - Police involvement and/or action

- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.

- There are support strategies in place for those reporting or affected by an online safety incident.

- Incidents should be logged on CPOMS.

- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.

- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).

- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - The Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
  - Staff, through regular briefings
  - Pupils, through assemblies/lessons

- Parents/carers, through newsletters, school social media, website
- Governors through regular safeguarding updates
- Local authority/external agencies, as relevant

7. School Actions

We may need to deal with incidents that involve inappropriate rather than illegal actions. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary/safeguarding procedures.

8. Online Safety Education

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum, this will be provided in the following ways:

- A planned online safety curriculum for all year groups
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Pupil needs and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PSHE; RHE; Literacy etc
- It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to Pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- Pupils should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside of the school.

Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.

- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- In lessons where internet use is pre-planned, it is best practice that Pupils 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

- Where Pupils are allowed to freely search the internet, staff should be vigilant in supervising the Pupils and monitoring the content of the websites / tools (including AI systems) the Pupils visit

- It is accepted that from time to time, for good educational reasons, Pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

9. Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the filtering and monitoring support provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and technical staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the filtering and monitoring support provider will have technical responsibility.

Checks on the filtering and monitoring system are carried out with the involvement of a senior leader, the Designated Safeguarding Lead, technical staff and a governor in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced.

9.1. Filtering

- The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering and monitoring. A member of the SLT and a governor are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined.

- The school manages access to content across its systems for all users and on all devices using the school's internet provision.

- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.

- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures.

- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.

- Filtering logs are regularly reviewed, and the Designated Safeguarding Lead is alerted to breaches of the filtering policy, which are then acted upon.

- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.

- Devices that are provided by the school have school-based filtering applied irrespective of their location.

- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.). Younger learners will use child friendly/age-appropriate search engines.

- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

9.2. Monitoring

The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users:

- The school monitors all network use across all its devices and services.

- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.

- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.

- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.

- Devices that are provided by the school have school-based monitoring applied irrespective of their location.

- Monitoring enables alerts to be matched to users and devices.

- Where AI –supported monitoring is used, the purpose and scope of this is clearly communicated.

10. Cyber Security

The DfE Cyber security standards for schools and colleges explains:

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage"

St Mary's Catholic Primary School has a Cyber Security Policy in place which covers the school's approach to security across our digital estate.

11. Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils, parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training

- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and governors

- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate