



St Michael & St Martin Catholic Primary School

Learning our faith, living our faith, loving our faith.

Online Safety Policy

Purpose and scope

We use technology to support learning while protecting children from harm. This policy applies to pupils, staff, governors, volunteers and visitors using school systems, and to online incidents outside school that affect pupil welfare or the school community. Our Catholic ethos requires respect for the dignity, privacy and safety of every person.

Online safety forms part of safeguarding, the curriculum and daily practice. It includes content, contact, conduct and commerce risks, such as harmful material, grooming, bullying, scams and financial exploitation. Filtering and monitoring support supervision and education; they do not replace them.

Responsibilities

- The Governing Board oversees online safety, seeks assurance about filtering and monitoring, and ensures appropriate resources and training. A nominated governor supports scrutiny without receiving unnecessary identifiable pupil information.
- The Headteacher ensures this policy is implemented and coordinates the DSL, senior leadership digital lead, IT support and Data Protection Officer.
- The DSL leads the safeguarding response to online concerns, reviews relevant monitoring alerts, and ensures concerns are recorded, assessed and referred when necessary.
- Staff supervise technology use, teach safe behaviour, know how to report a concern and follow the IT Acceptable Use Policy. Pupils receive age-appropriate support and are never blamed for seeking help.

Teaching and everyday practice

Curriculum and pupil voice

Online safety is taught progressively through computing, PSHE and other appropriate subjects. Lessons address safe searching, privacy, respectful communication, online relationships, misleading information, reporting routes, scams and the risks of AI-generated content. Pupils learn that they can tell any trusted adult and that harmful online behaviour can be reported even when it happens at home.

Teaching is adapted for age, development, SEND, language and vulnerability. EYFS and KS1 pupils use simple rules with adult support. KS2 pupils develop judgement about sharing, contact, privacy and digital footprints. Staff use pupil discussion and feedback to check understanding and improve provision.

Supervision and approved services

- Staff check planned websites, videos and online activities beforehand and supervise use appropriately. Search results and recommended content may change, so staff remain alert during lessons.
- Only approved platforms and applications are used. Approval considers safeguarding, age limits, privacy, accessibility, advertising, communication features and security.
- Pupils do not use personal accounts or access age-restricted services as part of lessons. School authorisation must comply with provider terms and applicable law.
- Remote learning uses approved accounts and professional communication routes. Staff protect private information, control meeting access and follow school rules for recording.
- Personal devices and photography follow the school Mobile Phone Policy and EYFS safeguards. Exceptions, including medical or accessibility needs, require documented authorisation and suitable controls.

Families and the wider community

The school shares practical online safety advice with families and explains reporting routes. Parents are encouraged to support age-appropriate use, discuss online experiences and report concerns. Parent acknowledgement supports shared expectations and does not transfer the school safeguarding responsibility to families.

Training

Induction covers online safety, reporting, acceptable use and filtering and monitoring responsibilities. Staff receive safeguarding updates and at least annual cyber security training. Governors receive safeguarding training appropriate to their responsibilities and updates needed to scrutinise online safety effectively.

Filtering and monitoring procedures

The Governing Board ensures appropriate filtering and monitoring arrangements. The DSL, digital lead and IT support review provision at least once each academic year and following significant changes or incidents. The school records the review, checks, findings and actions.

Review and checks

- Identify all internet-connected devices, networks and relevant locations, including school devices used off site. Confirm how protection operates on each and record any gaps.
- Assess pupil ages, SEND and other vulnerabilities; changing online risks; curriculum needs; and access available to different users. Avoid unreasonable restrictions on teaching while preventing access to harmful material.
- Use safe testing tools and provider-supported checks. Do not search for illegal material. Record date, device, location, result, action, owner and completion date.
- Check that blocked-site requests, attempted bypasses and technical faults can be reported. Only authorised staff may change filtering settings; requests and decisions are recorded.
- Confirm monitoring covers the risks identified, how alerts reach the school, response times, absence cover and out-of-hours limitations. Where provision does not offer continuous monitoring, communicate this clearly and assess the risk.

Alerts and escalation

IT support maintains the systems and escalates safeguarding alerts to the DSL or designated deputy promptly. The DSL assesses the context, risk and action needed. Staff report an immediate concern directly rather than assuming that an automated alert has reached the DSL. If a child is in immediate danger, contact emergency services and follow school safeguarding procedures.

Monitoring must be proportionate and transparent. Users are told about monitoring through acceptable use agreements and privacy notices. Logs and alerts are restricted to authorised people, retained for a justified period and handled under the Data Protection Policy. Monitoring access is not permission to browse confidential records without a legitimate reason.

School arrangements to complete before approval

Item	Confirmed arrangement
SLT digital lead and governor link	Nicola Duggan/ Remie Antao
IT provider and support contact	Infologix IT Services Ltd.
Filtering and monitoring services	SENSO
Alert recipients and absence cover	Nicola Duggan (DSL) Sabina Bell (DDSL)
Check frequency and annual review date	Half Termly Report
Out of hours arrangements and log retention	Infologix IT Services Ltd.

Responding to online concerns

Immediate staff response

- Listen calmly, reassure the pupil and do not promise secrecy. Do not investigate independently or ask a child to forward harmful content.
- Report to the DSL or a deputy immediately where there may be harm. Record facts, the pupil's words where relevant, time, platform and steps taken in the approved safeguarding recording system.
- Do not copy, download, print or share suspected sexual imagery of children. Do not view it unless there is a clear safeguarding reason and the DSL follows current specialist guidance.
- For technical compromise, stop using the affected service or device and contact IT support. Preserve relevant evidence safely; do not delete accounts or content before advice where this may compromise an investigation.

DSL assessment and follow up

The DSL considers immediate safety, grooming, exploitation, bullying, child-on-child abuse, threats, self-harm, sexual imagery and any discriminatory or extremist content. They decide on safeguarding referrals, police involvement, parental contact and support. Parents are normally informed unless doing so could increase risk or compromise a safeguarding response. The DSL records the rationale and follows local safeguarding procedures.

Children affected receive support and a proportionate response. Behaviour sanctions must not discourage disclosure. Allegations about staff follow the staff allegation and low-level concern procedures, including LADO consultation where appropriate. Concerns about the Headteacher are referred to the Chair of Governors through the school safeguarding arrangements.

Assurance and review

Leaders review incidents and themes, staff training, pupil understanding and the effectiveness of systems. Governors receive an anonymised report on assurance, risks and actions. Records include the annual filtering and monitoring review, checks, training and incident follow-up.

Guidance and related documents

[KCSIE 2026](#)

[DfE filtering and monitoring standard](#)

[DfE mobile phone guidance](#)

Read alongside the school Child Protection and Safeguarding Policy, Staff Code of Conduct, Behaviour Policy, Mobile Phone Policy and the other IT policies.