



ST MARY'S SCHOOL HAMPSTEAD

Online Safety POLICY

September 2026

Reviewed: September 2026
Next Review Date: September 2027

MISSION STATEMENT

St Mary's School seeks to provide an outstanding education firmly founded on the Catholic Faith.

Spiritual and moral principles are nurtured in a way that is reflected in daily life.

Within a happy and caring environment and based on the recognition of the dignity, worth and wellbeing of each child, high standards are expected. Intellectual development is emphasised and fostered along with the pursuit of academic excellence.

St Mary's values the unique contribution of every child within the school community.

St Mary's is inclusive and welcomes girls from all communities and faith backgrounds, or none, and believes that all benefit from the school's values.

St Mary's aims to encourage an active partnership between home, school, parish and the wider community.

1 Scope

This policy applies to all members of the school community (staff, volunteers or pupils) who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

This policy has regard to the following statutory guidance: Keeping Children Safe in Education (DfE, 2026); the Prevent Duty Guidance (Home Office, 2023), issued under section 29 of the Counter-Terrorism and Security Act 2015; the DfE's Generative AI: product safety expectations; and the UK Safer Internet Centre's Appropriate Filtering and Monitoring standards.

2 Objectives

2.1 ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices

2.2 provide staff and volunteers with the overarching principles that guide our approach to online safety

2.3 ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

3 Definitions

The school recognises the following categories of online risk:

- Content: exposure to illegal, inappropriate or harmful material, including pornography, extremist and radicalising content, disinformation, misinformation and conspiracy theories.
- Contact: harmful online interaction with others, including adults or peers seeking to exploit or groom, and interactions with generative AI systems that simulate human conversation.
- Conduct: personal online behaviour that causes or increases the risk of harm, including the making, sending or receiving of explicit images, including those digitally altered or wholly generated using artificial intelligence.
- Commerce: risks arising from commercial exploitation, including scams, financial harm and inappropriate advertising.

References to "nudes and semi-nudes" in this policy include images that are self-generated, digitally altered, or wholly generated using artificial intelligence, including so-called "deepfake" or "deep nude" content. The making, possessing or sharing of such images involving a person under 18 is treated with the same seriousness as other child protection concerns and is reported to the DSL immediately.

3 Guidance

3.1 The Headmistress will be responsible for the implementation of this policy. This includes taking overall responsibility for ensuring the standards related to monitoring and filtering are being met. This includes:

- ensuring filtering and monitoring systems are in place;
- making decisions regarding what is blocked or allowed and the reason for this are documented;
- reviewing the effectiveness of the provision; ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children;
- ensuring all staff understand their roles, are appropriately trained, follow policies, processes and procedures and act on reports and concerns;
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate;
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given;
- ensuring the school meets its safeguarding duty of care, including online safety;
- knowing and applying procedures for serious allegations involving staff;
- KCSIE requires them to:
 - Ensure that all staff 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 and regularly updated
 - Ensure that children be taught about safeguarding, including in relation to online safety
 - Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard

This policy should be read in conjunction with the filtering and monitoring checklist (360 Safe).

- 3.2 The DSL is the named senior leader responsible for the school's filtering and monitoring systems. The effectiveness of filtering and monitoring is formally reviewed at least once every academic year. Reviews include testing filtering across internet-connected devices and locations, and a written record is kept of: the date checks took place; the devices and environments tested; any issues identified; and the actions taken to address them.

Filtering and monitoring arrangements extend to generative AI tools used within the school, not solely to web browsing. Before any generative AI tool is deployed with pupils, it is assessed against the DfE's Generative AI: product safety expectations, covering age-appropriateness, data handling, content moderation and transparency of AI-generated outputs. Where a tool processes pupil data, a Data Protection Impact Assessment is completed and the Data Protection Officer is consulted before deployment.

Blocklists covering illegal content, including child sexual abuse material and terrorist or extremist material, cannot be disabled or altered by any user, including system administrators.

The DSL will:

- lead safeguarding, including online safety;
- maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security;
- compile logs of e-safety incidents;
- report to the Headmistress on recorded incidents;
- coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures;

- liaise with SLT, the Online Safety Governor, the IT provider and relevant external partners as required;
- review anonymised incident patterns and filtering/monitoring information;
- oversee and act on filtering and monitoring reports; safeguarding concerns; and checks to filtering and monitoring systems;
- with the nominated SLT Lead and the IT provider lead the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded;
- report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe);
- ensure appropriate support for learners with SEND.

Director of Innovation will act as E-Safety Co-ordinator, alongside the Designated Safeguarding Lead, and will:

- support the DSL regarding e-safety day to day;
- lead development and review of online safety documentation;
- coordinate awareness, staff confidence and reporting readiness through appropriate training;
- work with curriculum leads to map, embed and evaluate online safety education;
- liaise with IT and pastoral/support teams in maintenance of filtering and monitoring;
- maintain current knowledge of risks across content, contact, conduct and commerce;
- supporting and encouraging parents and carers to do what they can to keep their children safe online;
- liaise with school technical staff;
- advise on e-safety policy review and development; and
- ensuring that usernames, logins, email accounts and passwords are used effectively.

3.3 The Network Manager will have technical responsibility for:

- implementing and maintaining filtering and monitoring systems;
- providing filtering and monitoring reports;
- completing actions following concerns or checks to the system;
- the IT infrastructure and that it is not open to misuse or malicious attack;
- ensuring that users may only access the networks and devices through an enforced password protection policy; and
- ensuring that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse and is maintained.

The Network Manager will keep up to date with e-safety technical information in order to carry out their role.

3.4 Teaching and Support Staff will:

- maintain awareness of school e-safety policies and practices;
- ensure they have read, understood and signed the staff IT Acceptable Use Policy;
- report any suspected misuse or problem to the Headmistress or E-Safety Co-ordinator;
- ensure that all digital communications with pupils / parents / carers / fellow staff are on a professional level and conducted on school systems;
- where relevant e-safety is recognised in teaching activities and curriculum delivery;

- ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- monitor the use of digital technologies (including mobile devices, cameras etc.) during school activities
- supervise learner use of technology and follow procedures for online safety issue
- ensure that where the use of the internet 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.
- challenge harmful online behaviour and report concerns promptly;
- use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.

3.5 Child Protection

Those with over-arching responsibility for child protection (Designated Safeguarding Lead and deputies) should be trained in e-safety issues and aware of the implications that may arise from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate contact on-line with adults / strangers;
- potential or actual incidents of grooming; and
- cyber-bullying.

The Designated Safeguarding Lead has lead responsibility for safeguarding and online safety, including overseeing and acting on filtering and monitoring reports, safeguarding concerns and checks on the filtering and monitoring system.

The school's approach to online safety supports its Prevent duty obligations under the Counter-Terrorism and Security Act 2015. Filtering systems are configured to restrict access to material that promotes or glorifies terrorism or extremism. The school's Prevent risk assessment informs the configuration and review of filtering and monitoring arrangements. Staff receive Prevent awareness training (WRAP or equivalent), including guidance on recognising online indicators of radicalisation. Concerns relating to radicalisation or extremism are reported to the DSL through the same safeguarding pathway as any other online safety concern, with referral to the Channel programme where appropriate.

3.6 Pupils

- are responsible for using school digital technology systems, both in school and at home, in accordance with the School acceptable use policy;
- will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying; and
- will understand that the e-safety policy will include actions outside of school where related to school activities.
- use AI responsibly where it is embedded as part of an educational platform (e.g. Canva, Gemini/AI Mode on Google): protect original work, check accuracy and avoid plagiarism;

- understand that out-of-school behaviour may be addressed where it affects the school community.

3.7 Parents / Carers

- will be advised of e-safety policies through parents' evenings, newsletters, letters, school website, etc.;
- will be encouraged to support the School in the promotion of good e-safety practice; and
- should follow school guidelines on:
 - digital and video images taken at school events;
 - access to parents' sections of the school website / pupil records;
 - their children's / pupils' personal devices in the School (where this is permitted); and
 - their children's conduct and use of technology during any learning carried out via technology in their own home.

3.8 Governors

The Governor with responsibility for Safeguarding will also have strategic responsibility for online safety, including filtering and monitoring, and will need assurance that the standards are being met (this can be offered via the filtering and monitoring checklist and reports presented to the Safeguarding Governor following filtering and monitoring meetings).

Legal Requirements & Education Standards

References:

A: Handbook for the Inspection of Schools - The Regulatory Requirements, Part 3 (www.isi.net)

B: Reference Guide to the key standards in each type of social care service inspected by Ofsted (www.ofsted.gov.uk)

C: "Health and Safety at Work" Section H of the ISBA Model Staff Handbook,

D: "Health and Safety and Welfare at Work" Chapter N of the ISBA Bursar's Guide

E: "Insurance" Chapter K of the Bursar's Guide by HSBC Insurance Brokers Ltd

F: UK Council for Child Internet Safety (www.education.gov.uk/ukccis)

G: Cyber-bullying.org (www.cyberbullying.org)

H: Department for Education "Safer Working Practice for Adults who Work with Children and Young People" (www.education.gov.uk)