

St Monica's Catholic Primary School



Online Safety Policy 2026-2028

Approved by:	Governing Body	Date: July 2026
Created by:	Headteacher	
Next review due by:	July 2028	

Contents

Policy statement

1. Aims and scope
2. Legal and guidance framework
3. Online safety risks
4. Roles and responsibilities
5. Filtering and monitoring
6. Cyber security, data protection and access management
7. Online safety education
8. Safeguarding, reporting and responding to concerns
9. Sharing nudes and semi-nudes, AI-generated sexual imagery and sextortion
10. Online bullying, harassment and harmful communications
11. Generative artificial intelligence and emerging technology
12. Mobile phones, smartwatches and personal devices
13. Searching, examining and confiscating electronic devices
14. Remote education, live streaming and school-managed communications
15. Acceptable use of school technology
16. Staff use of technology, social media and work devices
17. Parents, carers and the wider community
18. Training
19. Recording, quality assurance and review
20. Links with other policies

[Appendix A: EYFS and Key Stage 1 acceptable use agreement](#)

[Appendix B: Key Stage 2 acceptable use agreement](#)

[Appendix C: Staff, governors, volunteers and visitors acceptable use agreement](#)

[Appendix D: Online safety incident and response record](#)

[Appendix E: Filtering and monitoring review record](#)

[Appendix F: Quick reporting guide for pupils and families](#)

Policy statement

At St Monica's Catholic Primary School, every child is created in the image and likeness of God and is entitled to learn, communicate and participate online with dignity, safety and respect. Technology can enrich learning, creativity and connection, but it can also expose children and adults to rapidly changing risks. Online safety is therefore part of safeguarding, not a separate technical issue.

The school takes a whole-school approach that combines education, supervision, clear expectations, appropriate filtering and monitoring, strong cyber security, staff training, accessible reporting routes and timely safeguarding action. Online incidents will be assessed on their facts and impact. Harm that begins outside school will be addressed where it affects a pupil, member of staff or the safe and orderly running of the school.

Core principle

Online harm is treated as seriously as harm that occurs face to face. A child will be listened to, protected and supported. Staff must not dismiss a concern because it happened outside school, on a personal device, within a game or app, or through artificial intelligence.

1. Aims and scope

This policy aims to:

- protect pupils, staff, governors, volunteers and visitors from online harm;
- ensure online safety is integrated across safeguarding, curriculum, behaviour, data protection and technology management;
- define clear responsibilities for governance, leadership, the DSL, IT support and all users;
- provide appropriate filtering and monitoring without unreasonably restricting teaching and learning;
- teach pupils the knowledge, judgement and reporting skills needed to use technology safely, respectfully and critically;
- set clear rules for school systems, accounts, devices, mobile phones, smart technology, social media and generative AI;
- identify, record, assess, escalate and learn from online safety incidents; and
- provide additional protection and reasonable adjustments for pupils with SEND, disabilities, medical needs, communication needs or other vulnerabilities.
- The policy applies to:
 - all pupils, including children in the Early Years Foundation Stage;
 - all staff, agency staff, contractors, governors, volunteers, visitors and trainee teachers;
 - school-owned, leased or managed devices, networks, accounts and services;
 - personal devices or accounts used on school premises, for school business or in a way that affects the school community;
 - remote education, educational visits, residential visits, clubs and school-organised activities; and
 - online conduct outside school where it raises a safeguarding concern, harms another person, disrupts education or may damage trust in the school.

2. Legal and guidance framework

This policy has been prepared with regard to current legislation and statutory or national guidance, including:

- the Children Acts 1989 and 2004 and the Education Act 2002;
- the Education and Inspections Act 2006 and Education Act 2011;
- the Equality Act 2010, including the Public Sector Equality Duty and the duty to make reasonable adjustments;
- the Human Rights Act 1998;
- the UK General Data Protection Regulation, Data Protection Act 2018 and Data (Use and Access) Act 2025;

- the Computer Misuse Act 1990, Sexual Offences Act 2003 and relevant criminal law relating to harassment, malicious communications, fraud and indecent images;
- the Counter-Terrorism and Security Act 2015 and current Prevent duty guidance;
- the Online Safety Act 2023 as part of the wider regulatory framework for online services;
- Keeping Children Safe in Education 2026, in force from 1 September 2026. KCSIE 2025 remains in force until 31 August 2026;
- Working Together to Safeguard Children 2026;
- Relationships Education, Relationships and Sex Education and Health Education statutory guidance introduced from 1 September 2026;
- Mobile Phones in Schools statutory guidance, which schools should follow from 1 September 2026;
- the DfE filtering and monitoring core standard and cyber security core standard;
- Teaching Online Safety in Schools and Searching, Screening and Confiscation guidance;
- UKCIS guidance on sharing nudes and semi-nudes, including AI-generated imagery;
- DfE guidance on generative AI in education, generative AI and data protection in schools, and generative AI product safety standards; and
- the national curriculum for computing and the Early Years Foundation Stage statutory framework.
- Where legislation or statutory guidance changes, the current legal requirement takes precedence. The school will update practice immediately where necessary and bring material policy amendments to the governing body.

3. Online safety risks

The school uses the four interrelated categories in KCSIE 2026:

Risk area	Examples
Content	Exposure to illegal, inappropriate or harmful content, including pornography, racism, misogyny, antisemitism, self-harm or suicide content, radicalisation, extremism, extreme violence, misinformation, disinformation and conspiracy theories.
Contact	Harmful interaction with people or generative AI applications that simulate people, including peer pressure, grooming, exploitation, impersonation, scams, sexual or criminal coercion and adults posing as children.
Conduct	Behaviour that causes or increases harm, including online bullying, harassment, abusive messages, doxxing, creation or sharing of explicit images, AI-generated images, deepfakes, exclusion from groups and misuse of another person's account or identity.
Commerce	Online gambling and gambling-like mechanics, inappropriate advertising, influencer marketing, phishing, fraud, in-app purchases, financial scams and pressure to pay or transfer money.

Risks can overlap. For example, a child may be contacted by an offender, coerced into creating an image, threatened with its distribution and asked for money. Staff must consider the complete safeguarding context rather than treating each element in isolation.

4. Roles and responsibilities

4.1 Governing Body

- Approve this policy and hold the headteacher to account for effective implementation.
- Ensure online safety is a running and interrelated theme across safeguarding, behaviour, curriculum, staff conduct, data protection, procurement and risk management.

- Ensure appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least once every academic year.
- Receive assurance that checks cover all internet-connected devices and relevant locations, that records are retained and that failures are escalated promptly.
- Review the DfE filtering and monitoring and cyber security standards with leaders, IT support and service providers.
- Ensure staff receive appropriate safeguarding and online safety training at induction, regular updates and at least annual refreshers.
- Ensure pupils are taught how to keep themselves and others safe online, with teaching adapted for age, SEND and vulnerability.
- Ensure governors receive safeguarding, online safety, filtering and monitoring and cyber security training appropriate to their responsibilities.
- Scrutinise incident themes, inequalities, emerging risks and the impact of actions without receiving unnecessary identifiable information.

4.2 Headteacher

- Provide visible leadership and ensure the policy is implemented consistently.
- Act as, or formally designate, the senior leadership team member responsible for filtering and monitoring.
- Ensure responsibilities, reporting routes and escalation arrangements are documented and understood.
- Ensure resources, contracts, staffing and training support effective online safety and cyber security.
- Ensure incidents involving staff are addressed under the staff code of conduct, low-level concerns, disciplinary or safeguarding procedures as appropriate.
- Ensure serious incidents are reported to the governing body, local authority, police, children's social care, data protection officer or other agencies where required.

4.3 Designated Safeguarding Lead (if different from the HT)

The DSL has lead responsibility for safeguarding and child protection, including online safety. The DSL will:

- understand the filtering and monitoring systems and processes used by the school;
- support the annual filtering and monitoring effectiveness review and the annual online safety risk assessment;
- receive and assess online safeguarding concerns, including child-on-child abuse, grooming, exploitation, sexual imagery, sextortion, radicalisation and AI-related harm;
- ensure records are accurate, timely, secure and linked to relevant safeguarding records;
- coordinate support and referrals, involving children and parents appropriately;
- liaise with IT support, the DPO, police, children's social care, Prevent partners and specialist services where necessary;
- provide or coordinate training and regular updates; and
- report themes, controls and required improvements to the headteacher and governing body.

4.4 Senior leader responsible for filtering and monitoring

- Own the operational effectiveness of filtering and monitoring provision.
- Chair or coordinate the annual effectiveness review with the DSL and IT support.
- Ensure filtering works appropriately on all internet-connected devices and in all relevant locations, including mobile or app-based technology where applicable.
- Ensure monitoring alerts are reviewed by appropriately trained staff within agreed timescales.
- Maintain records of testing, decisions, incidents, overrides and actions.
- Ensure over-blocking does not unreasonably restrict teaching, learning or access to safeguarding information.
- Escalate material weaknesses and ensure remedial action is tracked to completion.

4.5 IT support and service providers (currently Agylysis)

- Implement and maintain approved filtering, monitoring, account security, device management, backups, patching and malware protection.

- Provide leaders with understandable reports and assurance, not merely technical data.
- Test controls in cooperation with the school and respond promptly to faults or safeguarding concerns.
- Apply the principle of least privilege and maintain accurate hardware, software, account and information asset records.
- Preserve relevant logs and evidence when an incident occurs and support lawful investigation.
- Notify the school promptly of security incidents, vulnerabilities or service changes that may affect safeguarding or data protection.

4.6 All staff, contractors and volunteers

- Read, understand and follow this policy, the acceptable use agreement and safeguarding procedures.
- Use only approved devices, accounts, platforms and applications for school business.
- Maintain professional boundaries and model safe, respectful and responsible technology use.
- Know how to report a safeguarding concern, a filtering or monitoring failure, a suspicious message, a data breach or a lost device.
- Report concerns immediately to the DSL or a deputy. Technical faults must also be reported through the approved IT route.
- Never investigate a safeguarding concern beyond what is necessary to establish immediate safety and pass on the report.
- Never promise confidentiality, blame a child or ask a child to delete evidence.
- Respond to online sexual harassment and child-on-child abuse with an attitude that it could happen here.

4.7 Pupils

- Follow the age-appropriate acceptable use agreement and classroom instructions.
- Use school technology for authorised learning purposes.
- Treat other people with respect and do not create, request, share or forward harmful content.
- Keep passwords and personal information private.
- Report anything worrying, unsafe or inappropriate to a trusted adult, even if they are unsure, embarrassed or worried about getting into trouble.
- Do not attempt to bypass security, filtering, monitoring or access controls.

4.8 Parents and carers

- Support the school's acceptable use and mobile phone arrangements.
- Discuss safe, respectful and balanced technology use at home and use age-appropriate parental controls where appropriate.
- Report concerns promptly and preserve relevant evidence without redistributing harmful content.
- Use the school office for urgent contact during the school day rather than contacting a pupil's personal device.
- Work with the school where a child needs additional support, a reasonable adjustment or a safeguarding response.

5. Filtering and monitoring

The school will do all that it reasonably can to limit pupils' exposure to online risk through school systems while preserving appropriate access to education, information and safeguarding support.

5.1 Core arrangements

- Filtering will block harmful and inappropriate content, including known child sexual abuse material, terrorist content, malicious websites and categories identified through the school's risk assessment.
- Monitoring will identify and alert the school to behaviour or content associated with the four online risk categories.
- Controls will apply to school networks and school-managed devices. Where mobile or app-based technology can bypass network filtering, additional device or application controls will be considered.
- Access rights and filtering profiles will be proportionate to age, role, vulnerability and curriculum need.

- No user may attempt to bypass controls. Educational overrides may be authorised only through the documented process and must not expose pupils to unmanaged risk.
- Monitoring information will be accessed only by authorised staff and handled as safeguarding and personal data.

5.2 Annual effectiveness review and checks

At least once every academic year, the responsible senior leader, supported by the DSL and IT support, will review effectiveness. The review will:

- test that filtering works appropriately across all internet-connected device types, user groups and relevant school locations;
- check that monitoring alerts are generated, received, triaged, escalated and resolved as intended;
- consider pupil age, SEND, vulnerabilities, usage patterns, remote access and emerging risks;
- review blocked and allowed categories, exceptions, over-blocking and curriculum impact;
- consider whether generative AI and new applications are covered by filtering and monitoring;
- review contracts, data flows, retention, access permissions and supplier assurance;
- record findings, actions, owners, deadlines and completion; and
- report assurance and material weaknesses to the governing body.

6. Cyber security, data protection and access management

Cyber security is part of safeguarding because loss of access, exposure of personal information, account compromise or malicious content can place children and adults at risk.

- School data and communications must be processed only through approved systems and in accordance with the Data Protection Policy and privacy notices.
- Users must use strong, unique passwords or passphrases and must not share credentials. Multi-factor authentication will be used where available and proportionate.
- Access will be limited to what is required for the user's role and removed promptly when roles change or employment ends.
- School devices will be encrypted where appropriate, supported, patched and protected against malware.
- Personal data must not be copied to personal email, unapproved cloud storage, messaging apps, removable media or personal AI tools.
- Backups will be maintained, protected from unauthorised alteration and tested as part of business continuity arrangements.
- Suspicious emails, login prompts, QR codes, attachments, links or requests for payment or information must be reported and not actioned until verified.
- Lost or stolen devices, accidental disclosure, ransomware, account compromise and other security incidents must be reported immediately to the headteacher, IT support and DPO as appropriate.
- The school will maintain and test a cyber incident response plan and will consider reporting serious incidents to relevant authorities.

7. Online safety education

Online safety will be taught through Relationships and Health Education, computing, PSHE, safeguarding education and other curriculum opportunities. Teaching will be planned, progressive, age-appropriate, factual and responsive to local and emerging risk.

7.1 By the end of primary school, pupils will be taught

- that the same standards of respect, kindness, consent and responsibility apply online and face to face, including where people are anonymous;
- how to recognise harmful content, harmful contact, manipulation, grooming, pressure and unsafe relationships, and how to report concerns;
- that people and AI applications may pretend to be someone or something they are not;

- that most major social media services have a minimum joining age, commonly 13, and that age limits are protective safeguards;
- how to protect personal information through privacy, security and location settings;
- that images, words and information can be copied, altered and circulated beyond the sender's control;
- how to resist pressure to share information or images and how to seek help without fear of blame;
- how to recognise misinformation, disinformation, conspiracy theories, manipulated media, deepfakes and AI-generated content;
- how advertising, influencers, algorithms and recommendation systems may shape what they see and encourage spending or prolonged use;
- the risks of scams, phishing, online gambling and gambling-like features within games;
- how online activity can affect sleep, concentration, emotional wellbeing, body image, relationships and physical health;
- how to respond to online bullying, prejudice, misogyny, racism, antisemitism, hate, radicalisation and extremist content;
- where and how to obtain help from trusted adults, the school, emergency services and specialist reporting services.

7.2 Teaching approach

- Staff will establish a safe classroom climate and avoid asking pupils to disclose personal experiences publicly.
- Resources and external visitors will be checked for accuracy, age suitability, bias, safeguarding quality and alignment with school values.
- Teaching will be adapted for pupils with SEND, communication needs, trauma, limited digital literacy or other vulnerabilities.
- Staff will avoid unnecessarily graphic or instructional detail, particularly in relation to self-harm, suicide, sexual content or criminal methods.
- Any disclosure or concern arising during teaching will be handled under safeguarding procedures.

8. Safeguarding, reporting and responding to concerns

8.1 Reporting

- Pupils may report to any trusted adult verbally, in writing or through an agreed accessible method.
- Staff must listen calmly, take the child seriously, avoid leading questions, establish immediate safety and report to the DSL without delay.
- A concern must be recorded in the school's safeguarding system as soon as possible using the child's own words where relevant.
- If a child is in immediate danger, staff will contact emergency services and follow safeguarding procedures.
- Technical incidents, security failures and data breaches must also be reported through the relevant IT and data protection routes.
- Anonymous reports will be assessed and acted upon where possible, although anonymity may limit the school's ability to investigate or provide feedback.

8.2 Initial response and assessment

The DSL or appropriate senior leader will consider:

- the immediate safety and welfare of all children involved;
- the nature, severity, reach, persistence and likely impact of the content or conduct;
- whether the concern involves abuse, exploitation, coercion, discrimination, a criminal offence, radicalisation, a data breach or risk to life;
- the child's age, development, SEND, vulnerabilities, wishes and understanding;
- whether evidence needs to be preserved and whether a device or account should be secured;
- whether parents should be informed and whether doing so could increase risk;
- whether police, children's social care, Prevent, the DPO, CEOP or another specialist service should be involved;

- what support, safety planning, education and proportionate consequences are required.
- The school will not require a child to confront another child, participate in restorative work or apologise where this would be unsafe, inappropriate or contrary to their wishes and welfare.

9. Sharing nudes and semi-nudes, AI-generated sexual imagery and sextortion

This section includes nude or semi-nude images, videos or live streams involving a person under 18, whether self-generated, created by another person, digitally altered or wholly generated using AI. It also includes threats to share images and financially motivated sexual extortion.

Staff must not view or copy imagery

A member of staff who receives a report must not ask to see, view, copy, print, save, forward, upload, screenshot or delete the image. The device should not be passed around. The concern must be reported immediately to the DSL, who will follow current UKCIS and safeguarding guidance.

- Taking, possessing, sharing or generating indecent or sexual images of a person under 18 may be a criminal offence, including where AI has been used.
- The child's welfare is the immediate priority. A child who asks for help will be reassured that they have done the right thing and will not be blamed for reporting.
- The DSL will undertake an initial review and decide whether police or children's social care must be involved, following current UKCIS guidance.
- Parents will normally be informed unless doing so may place a child at additional risk or undermine a safeguarding or police response.
- The school will preserve evidence lawfully and will not ask a child or parent to redistribute imagery to prove what happened.
- Support will address emotional wellbeing, peer impact, online removal and reporting, account security and ongoing safety.
- Any behaviour consequences will be proportionate and informed by safeguarding, coercion, consent, age, vulnerability and the circumstances of each child.

10. Online bullying, harassment and harmful communications

Online bullying may occur through messages, group chats, games, shared documents, social media, altered images, impersonation, exclusion, doxxing or repeated unwanted contact. Bullying usually involves repetition and an imbalance of power, but a single online act can be repeatedly viewed or shared and can cause serious harm. It will not be dismissed because it occurred once or outside school.

- Reports will be handled under the Anti-Bullying, Positive Behaviour and Relationships, and safeguarding policies as appropriate.
- Prejudice-related abuse, misogyny, sexual harassment, threats, hate content and discriminatory language will be identified and addressed explicitly.
- The school will consider the needs and safety of the harmed child, the child responsible for the behaviour and any witnesses or bystanders.
- The response may include safeguarding action, parental involvement, removal or reporting of content, account security measures, education, support, proportionate consequences and external referral.
- Staff will avoid describing harmful conduct as banter, a joke or a normal part of growing up.

11. Generative artificial intelligence and emerging technology

Generative AI can support education, but it can also produce inaccurate, biased, unsafe or fabricated material; expose personal data; imitate human contact; create deepfakes; enable cheating; and generate harmful or sexualised content. AI use must be purposeful, approved, transparent and supervised.

11.1 School approval and risk assessment

- Only school-approved AI tools may be used for school business or with pupils.
- Before approving a tool, the school will consider educational need, age restrictions, safeguarding, filtering and monitoring, data protection, security, bias, accessibility, intellectual property, supplier terms, retention and human oversight.
- The DPO and IT lead will be consulted where personal data may be processed. A data protection impact assessment will be completed where required.
- Pupil-facing use will have appropriate safeguards, close adult supervision and suitable safety settings.
- The school will prefer products aligned with DfE generative AI product safety standards.

11.2 Rules for use

- Personal, safeguarding, special category or confidential information must not be entered into an AI tool unless the use is specifically approved and legally compliant.
- AI output must be checked for accuracy, bias, appropriateness and copyright or attribution issues before use.
- Staff remain professionally accountable for materials, decisions, feedback and communications produced with AI support.
- Pupils must not use AI to impersonate, humiliate, sexualise, threaten, deceive or exploit another person, or to bypass learning expectations.
- Where AI has materially contributed to school work, its use should be acknowledged in line with teacher instructions and school expectations.
- Suspected AI-generated harmful content will be treated according to its impact and safeguarding context, not as a lesser or unreal form of harm.

12. Mobile phones, smartwatches and personal devices

St Monica's is a mobile phone-free school throughout the school day. This includes lessons, movement around school, breaktimes, lunchtime, clubs and other activities taking place within the normal school day. The term includes phones and smart technology capable of messaging, notifications, recording audio or video, accessing the internet or performing similar communication functions.

12.1 Pupil arrangements

- Pupils should not bring a mobile phone, smartwatch or similar personal communication device to school unless a parent has requested this for travel, safety or another agreed reason.
- Year 6 pupils with permission may bring a phone to school. Any permitted device must be switched off and handed to the school office on arrival, or stored through another arrangement authorised by the headteacher. It may be collected at the end of the school day.
- Parents who need to contact a child during the day must contact the school office.
- The school may apply proportionate sanctions, including confiscation, where a pupil breaches these rules.
- The school does not accept responsibility for avoidable loss or damage to an unauthorised device, although staff will handle any confiscated item lawfully and carefully.

12.2 Exceptions and reasonable adjustments

The school will consider individual exceptions where required by law or justified by the pupil's circumstances, including disability, medical need, SEND, safeguarding, travel arrangements or young-carer responsibilities. Any exception will specify the purpose, times, location, supervision and permitted functions. It will not create unrestricted use.

12.3 Staff devices

- Staff should not use personal phones for personal reasons in front of pupils during the school day.
- Limited professional use may be authorised, for example for multi-factor authentication, an emergency, a specific educational activity or an approved school system.

- Personal devices must not be used to photograph, record or communicate with pupils except under an explicitly approved arrangement consistent with safeguarding and data protection procedures.

13. Searching, examining and confiscating electronic devices

Searching and confiscation will be undertaken only in accordance with current DfE guidance, the school's Behaviour and Relationships Policy and the law.

- Only the headteacher or a member of staff authorised by the headteacher may conduct a search within the scope of the school's legal powers and published rules.
- Before a search, staff will consider urgency, safeguarding risk, the pupil's age, SEND and vulnerability, explain the process and seek cooperation where appropriate.
- An authorised person may examine data on a confiscated device only where there is a lawful and proportionate good reason.
- Material that may be evidence of an offence must not be deleted and the device or evidence will be secured for police advice or handover.
- A member of staff must not view a suspected nude or semi-nude image of a child. The device must be secured and referred immediately to the DSL.
- Any deletion of material will be lawful, proportionate and documented. Safeguarding and evidential considerations take priority.
- Complaints about searching or confiscation will be addressed through the school complaints procedure.

14. Remote education, live streaming and school-managed communications

- Only approved platforms, accounts and devices will be used for remote education and school-managed communication.
- Staff and pupils must use professional language, appropriate backgrounds and agreed functions. Private one-to-one communication outside approved systems is not permitted.
- Parents will be told what pupils are expected to access, who they may interact with and how concerns can be reported.
- Sessions will not be recorded, photographed or redistributed unless this has been authorised, communicated and is legally compliant.
- Attendance, conduct and safeguarding concerns arising remotely will be handled under the same standards as in-person activity.
- The school will consider accessibility, home circumstances, data protection, supervision and safe alternatives when planning remote activity.

15. Acceptable use of school technology

- All users must follow the relevant acceptable use agreement.
- School systems are provided primarily for education, safeguarding, administration and authorised professional activity.
- Users must not access, create, store or share illegal, abusive, discriminatory, sexual, violent, extremist or otherwise harmful material except where authorised staff must handle information for safeguarding or legal purposes.
- Users must not disable security, install unapproved software, connect unauthorised hardware, scan or probe systems, use another person's account or deliberately consume excessive resources.
- The school may monitor use of its systems lawfully and proportionately for safeguarding, security, compliance and operational purposes.
- Privacy will be respected, but users should not expect personal privacy when using school-managed systems or accounts.
- Breaches will be considered under safeguarding, behaviour, staff conduct, disciplinary, data protection or legal procedures as appropriate.

16. Staff use of technology, social media and work devices

- Staff must maintain professional boundaries online and must not communicate with pupils through personal social media, personal messaging accounts or gaming accounts.
- Staff must not accept or initiate social media connections with current pupils. Communication with former pupils must remain professionally appropriate and comply with the staff code of conduct.
- Confidential school information must not be discussed on personal accounts or informal messaging groups.
- Images or recordings of pupils may be taken only on approved devices and for an authorised purpose, with relevant permissions and secure storage.
- Work devices must be protected against unauthorised access, kept updated, encrypted where provided, locked when unattended and not shared with family or friends.
- Staff must not use public or insecure Wi-Fi for sensitive work without approved protection.
- School records must not be retained on a personal device after the authorised purpose has ended.
- Concerns about a member of staff's online conduct must be reported under the safeguarding allegations, low-level concerns or whistleblowing arrangements as appropriate.

17. Parents, carers and the wider community

- The school will provide regular, practical online safety information through communications, meetings, workshops or the school website.
- Parents will be informed about filtering and monitoring arrangements in a way that supports understanding without exposing security-sensitive detail.
- The school will signpost trusted guidance on age restrictions, parental controls, scams, gaming, social media, harmful content, image sharing, AI, screen use and reporting routes.
- Parents should contact the school promptly about online incidents affecting a pupil and should not confront another child or family online.
- Visitors, contractors and community users of school technology must follow this policy and the relevant acceptable use agreement.

18. Training

- All new staff will receive safeguarding and child protection training at induction, including online safety and responsibilities for filtering and monitoring.
- All staff will receive regular safeguarding and online safety updates and a formal refresher at least annually.
- Training will reflect emerging risks, local incidents, AI, sexual imagery, sextortion, misinformation, radicalisation, scams, cyber security and the needs of vulnerable pupils.
- The DSL will refresh knowledge and skills at regular intervals and at least annually, in addition to formal DSL training requirements.
- Governors will receive training sufficient to challenge and assure leaders on online safety, filtering and monitoring and cyber security.
- Relevant IT staff and service providers must understand safeguarding expectations and escalation routes, not solely technical duties.
- The school will evaluate training through staff feedback, audits, incident learning and assurance checks.

19. Recording, quality assurance and review

- Online safeguarding concerns will be recorded within the school's safeguarding system. Technical incidents, security events and data breaches will also be recorded in the appropriate operational systems.
- Records will distinguish allegation, evidence, professional assessment, decision, action, rationale, outcome and follow-up.
- The DSL and leaders will review patterns, including protected characteristics, SEND, vulnerability, year group, platform, location, time and repeated involvement, while avoiding unfair assumptions.

- Lessons from incidents will inform curriculum, supervision, filtering, monitoring, staff training, parent engagement and risk controls.
- The school will review its online safety approach and risk assessment at least annually and sooner after a serious incident, major technology change or new statutory requirement.
- The governing body will review the policy annually during the 2026-2028 policy period. The next scheduled review is July 2027.

20. Links with other policies

- Child Protection and Safeguarding Policy
- Positive Behaviour and Relationships Policy
- Anti-Bullying Policy
- Data Protection Policy and privacy notices
- Artificial Intelligence Policy
- Staff Code of Conduct and low-level concerns procedure
- SEND and Equality policies
- Acceptable Use and ICT procedures
- Records Management and Data Breach procedures
- Whistleblowing Policy
- Complaints Procedure
- Remote Education

Appendix A: EYFS and Key Stage 1 acceptable use agreement

Child-friendly agreement: using computers, tablets and the internet safely at St Monica's.

- I will ask an adult before I use a device or go online.
- I will use the websites, apps and activities my teacher has chosen.
- I will be kind and respectful when I use technology.
- I will keep my name, address, location, passwords and other private information safe.
- I will not take or share a photo, video or recording without permission.
- I will tell a trusted adult straight away if I see something worrying, upsetting, confusing or unkind.
- I will tell an adult if someone asks me to keep an unsafe secret, share information or send an image.
- I will not try to change settings, use another person's account or get around the school's safety controls.
- I will look after school equipment and report anything broken or not working.
- I understand that adults may check how school devices and internet are used to help keep everyone safe.

Name of pupil	Class
Pupil signature or mark	Date
Parent/carers signature	Date

Parent/carers agreement: I have discussed these rules with my child and will support the school's online safety and mobile phone arrangements.

Appendix B: Key Stage 2 acceptable use agreement

When I use school technology, accounts or the internet, I will:

- use them responsibly, respectfully and only for an authorised purpose;
- follow staff instructions and use only approved websites, apps and AI tools;
- keep passwords private and report any account I think has been compromised;
- protect personal information, images and location details;
- check information carefully and remember that online content, people and AI responses may be false or misleading;
- ask before taking, using or sharing an image, video, audio recording or another person's work;
- tell a trusted adult immediately about harmful content, contact, pressure, bullying, scams, sexual images or anything that makes me worried;
- remember that I will not be blamed for asking for help;
- use respectful language and not exclude, threaten, embarrass, impersonate or harass another person;
- not create, request, keep, forward or share nude or sexual images, including AI-generated images;
- not install software, change settings, use someone else's account or bypass filtering, monitoring or security;
- not use a personal phone, smartwatch or communication device during the school day unless the school has agreed an exception;
- look after equipment, log off when finished and report damage or technical problems.

I understand that school systems may be monitored for safeguarding and security, and that concerns or misuse may be addressed under school policies.

Name of pupil	Class
Pupil signature	Date
Parent/carers signature	Date

Appendix C: Staff, governors, volunteers and visitors acceptable use agreement

I agree that I will:

- use only approved accounts, systems, storage, devices, platforms and AI tools for school business;
- protect credentials, use multi-factor authentication where provided and lock devices when unattended;
- process personal data only for an authorised purpose and in accordance with school policy;
- maintain professional boundaries and use approved channels for communication with pupils and families;
- use approved equipment for pupil images, recordings and school records;
- report safeguarding concerns immediately to the DSL and report filtering, monitoring, cyber security or data protection incidents through the correct route;
- not view, copy, save, forward or delete suspected nude or semi-nude imagery involving a child;
- not attempt to bypass security or access data, accounts or systems beyond my authorisation;
- not install unauthorised software or connect unauthorised equipment;
- check AI output and remain accountable for all professional decisions and materials;
- not enter personal, confidential or safeguarding information into an unapproved AI or online service;
- not use school technology to access, create or distribute illegal, discriminatory, abusive, sexual, extremist or otherwise harmful material;
- understand that use of school-managed systems may be monitored lawfully and proportionately.

Name	Role
Signature	Date

Appendix D: Online safety incident and response record

Field	Record
Date and time reported	
Person reporting and contact details	
Pupil(s), staff or others involved	
How the concern came to light	
Child's words / factual account	
Platform, device, account or location	
Risk category	Content / Contact / Conduct / Commerce
Immediate safety action	
Evidence preserved and location	Do not attach or reproduce illegal sexual imagery
DSL / senior leader informed	
Parents informed	Yes / No / Deferred - rationale
External advice or referral	Police / Children's social care / CEOP / Prevent / DPO / IT / Other
Decision and rationale	
Support and safety plan	

Field	Record
Behaviour or employment response	
Content removal / account security action	
Follow-up date and outcome	
Learning and control improvements	
Completed by and date	

Appendix E: Filtering and monitoring review record

Complete at least once every academic year and after a material system change or serious incident.

Review area	Finding / evidence
Review date and period covered	
Responsible senior leader	
DSL and IT support participants	
Systems, providers and contracts reviewed	
Networks and locations tested	Classrooms, offices, shared areas, remote access and other relevant locations
Device types and user profiles tested	Staff, pupil, visitor, managed mobile/app devices and accessibility profiles
Filtering tests and results	Harmful content, over-blocking, curriculum access and safeguarding resources
Monitoring tests and results	Alerts generated, received, triaged, escalated, recorded and resolved
AI services and emerging technology	Coverage, controls, age restrictions and monitoring
Prevent risk assessment alignment	
Data protection and access controls	Permissions, logs, retention, supplier access and confidentiality
Incidents and trend analysis	
Staff knowledge and escalation routes	
Pupil and parent feedback	
Strengths	
Weaknesses and risk rating	
Actions, owners and deadlines	
Completion verified	
Reported to governing body	Date and outcome

Appendix F: Quick reporting guide for pupils and families

Tell someone

Tell a trusted adult at school or at home. You can report even when you are unsure, embarrassed, involved in what happened or worried that you broke a rule. Asking for help is the right thing to do.

What to do

- Stop responding to the person or account if it is safe to do so.
- Do not forward harmful, sexual or illegal content to another person.
- Keep useful evidence such as usernames, dates, messages or web addresses, but do not screenshot or copy a sexual image of a child.
- Block and report the account or content using the platform's tools where appropriate.
- Change passwords and secure the account if access may have been compromised.
- Contact the school promptly when the incident affects a pupil or the school community.
- Call 999 if someone is in immediate danger. Contact police on 101 for non-emergency criminal concerns.
- Use the CEOP Safety Centre to report online sexual abuse or grooming. Trusted removal and reporting support can also be accessed through services signposted by the school.

What the school will do

- listen without blaming;
- check immediate safety;
- record and assess the concern;
- involve parents and agencies where appropriate;
- support the child and take steps to prevent further harm;
- explain what can be shared about the response while protecting confidentiality.

End of policy