ST MARGARET MARY'S CATHOLIC PRIMARY SCHOOL

ONLINE SAFETY AND ACCEPTABLE USE POLICY

2026–2027

Mission Statement

"In St Margaret Mary's School we welcome everyone into our community in order to live, love and learn together in the light and example of the life of Christ."

Policy owner	Headteacher / Designated Safeguarding Lead / Computing Lead
Approved by	Governing Body
Approval date	September 2026
Review date	July 2027, or earlier following a significant incident or change
Applies to	Pupils, staff, governors, volunteers, visitors, contractors and all users of school systems

Policy status and key documents

This policy forms part of the school's safeguarding arrangements. It should be read with the Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, Data Protection Policy, Privacy Notices, Mobile Phone Policy, Social Media Policy, Remote Learning arrangements, Whistleblowing Policy and disciplinary procedures.

> **Effective date:** Keeping Children Safe in Education (KCSIE) 2025 remains in force until 31 August 2026. This policy is written for the 2026–27 academic year and reflects KCSIE 2026, which takes effect on 1 September 2026.

Legislation and statutory guidance

- Education Act 2002, including the duty to safeguard and promote children's welfare;
- Children Acts 1989 and 2004 and Working Together to Safeguard Children;
- Keeping Children Safe in Education 2026;
- UK General Data Protection Regulation, Data Protection Act 2018 and Data (Use and Access) Act 2025;
- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988;
- Equality Act 2010 and the Public Sector Equality Duty;
- Counter-Terrorism and Security Act 2015 and Prevent Duty Guidance;
- Human Rights Act 1998;
- Protection from Harassment Act 1997, Communications Act 2003 and Malicious Communications Act 1988;
- Voyeurism (Offences) Act 2019 and relevant provisions concerning sexual images and intimate-image abuse;
- Online Safety Act 2023, where relevant to the services and platforms used by the school;
- DfE filtering and monitoring, cyber-security, mobile-phone and generative-AI guidance.

Contents

1. Purpose and principles
2. Scope
3. Roles and responsibilities
4. Education and training
5. Filtering and monitoring
6. Acceptable use
7. Unacceptable use
8. Generative artificial intelligence
9. Data protection and confidentiality
10. Email, cloud services and communication
11. Mobile, smart and personal devices
12. Images, video and livestreaming
13. Social media and professional boundaries
14. Cyber security
15. Online safeguarding concerns
16. Incident response and sanctions
17. Equality, SEND and accessibility
18. Monitoring, review and record keeping
Appendix A: Staff AUP
Appendix B: KS2 pupil AUP
Appendix C: EYFS/KS1 pupil agreement
Appendix D: Visitors, volunteers and contractors

1. Purpose and principles

Technology is an important part of teaching, learning, communication and school administration. The school will provide a safe digital environment while enabling pupils to develop knowledge, confidence, critical thinking and responsible online behaviour.

- Safeguarding children online is part of safeguarding children generally and is everyone's responsibility.
- Online-safety decisions will be child-centred, proportionate, inclusive and informed by the school's risk profile.
- Filtering and monitoring support safeguarding but do not replace education, supervision or professional judgement.
- Pupils will be taught to recognise risk, behave respectfully and seek help.
- Use of school technology is a privilege and must support education, safeguarding and legitimate school business.

2. Scope

This policy applies:

- to all pupils, employees, governors, volunteers, visitors, contractors, supply and agency staff;
- to school-owned, leased or managed devices, networks, accounts, applications and cloud services;
- to personal devices connected to school systems or used for school business;
- on and off the school site, including remote learning, school trips and school devices taken home;
- to online conduct outside school where it affects a pupil's welfare, the school community, staff professional boundaries or the safe running and reputation of the school.

3. Roles and responsibilities

Role	Responsibility
Governing Body	Has overall strategic responsibility; appoints a responsible governor; receives assurance; approves this policy; ensures filtering and monitoring standards are met and reviewed.
Headteacher / SLT digital lead	Implements the policy; allocates resources; documents decisions about access; oversees reports, training, procurement, incidents and disciplinary action.
Designated Safeguarding Lead	Leads online safeguarding; understands filtering and monitoring arrangements; checks relevant reports and high-risk alerts; ensures concerns are recorded, assessed and acted upon.
Computing / Online Safety Lead	Supports curriculum delivery, age-appropriate pupil guidance, staff awareness and annual policy review; works with the DSL, DPO and IT support.
Data Protection Officer	Advises on lawful processing, DPIAs, privacy notices, breaches, AI and EdTech procurement, information sharing and data-protection complaints.
IT support/provider	Maintains secure systems; implements filtering and monitoring; completes and records checks; supplies understandable reports; promptly escalates technical and safeguarding concerns.
All staff	Follow this policy; supervise pupils; maintain professional boundaries; undertake training; report safeguarding, cyber and data concerns without delay.

Role	Responsibility
Pupils	Use technology safely, respectfully and honestly; protect accounts and personal information; tell a trusted adult about concerns.
Parents and carers	Support the school's expectations, discuss online safety at home and report relevant concerns.

4. Education and training

- Online safety will be taught through a planned, age-appropriate curriculum and reinforced whenever technology is used.
- Teaching will address content, contact, conduct and commerce risks, including misinformation, scams, grooming, coercion, cyberbullying, pornography, radicalisation, misogyny, deepfakes and AI-generated material.
- Pupils will learn about privacy, consent, healthy relationships, reporting routes, copyright, digital footprints and the safe sharing of images.
- Staff, pupils and at least one governor will receive appropriate cyber-security and online-safety training at least annually. New, temporary and supply staff will receive relevant information during induction.
- Staff will receive regular updates on filtering and monitoring, emerging risks and how to report concerns.

5. Filtering and monitoring

The Governing Body will ensure that the school has appropriate filtering and monitoring systems that reflect the age, needs and risk profile of pupils and do not unreasonably restrict teaching and learning.

5.1 Minimum arrangements

- Filtering will address illegal, inappropriate and potentially harmful text, images, audio, video, apps and AI-generated content.
- As a minimum, filtering will be tested for illegal child sexual abuse material, unlawful terrorist content and adult content.
- Different access profiles will be used for pupils, staff and guests where appropriate; a single blanket profile will not be assumed suitable.
- Monitoring will combine appropriate technical measures with active classroom supervision.
- Users must be identifiable wherever reasonably possible. Shared or guest accounts will be restricted and controlled.
- Monitoring reports will be reviewed at least weekly. High-risk safeguarding, malicious or technical alerts will be escalated immediately under the agreed response process.
- Filtering and monitoring will apply to all relevant school-managed devices and services, including devices used off-site where technically possible and appropriate.
- All users will be informed that use may be filtered, logged and monitored. Monitoring will be lawful, proportionate, transparent and limited to legitimate safeguarding, security and operational purposes.

5.2 Review and checks

- SLT, the DSL and IT support, with the responsible governor, will review effectiveness at least once each academic year.
- The review will consider pupil risk profiles, SEND, EAL, curriculum needs, BYOD, remote use, new devices, apps, AI tools, incidents, system limitations and changes to safeguarding risks.

- Checks will cover all relevant internet-connected devices, services, user groups and locations. They will also be completed after material system changes and before new devices or services are issued.
- A written log will record the date, person completing the check, what was tested, findings and resulting actions.
- Requests to block or unblock content will be authorised, documented and reviewed. Staff must never attempt to bypass filtering.

6. Acceptable use

Users may use school technology only for authorised educational, professional or limited approved personal purposes. Users must:

- use their own account and keep authentication details secure;
- communicate respectfully and use approved school systems;
- protect personal, safeguarding and confidential information;
- check recipients and attachments before sending messages;
- credit sources and comply with copyright and licensing;
- store school work and records only in approved locations;
- lock or sign out of devices when unattended;
- report accidental access, suspicious messages, lost devices, security weaknesses and harmful content promptly;
- follow staff instructions, age restrictions and the terms of approved services.

7. Unacceptable use

Users must not:

- create, view, search for, save, send or share illegal, abusive, sexual, hateful, extremist or otherwise harmful material;
- bully, harass, threaten, discriminate against, impersonate or deliberately embarrass another person;
- make or share nude or semi-nude images, sexualised deepfakes or other intimate images;
- attempt to access another person's account, data or communications;
- circumvent filtering, monitoring, security controls or device management, including through VPNs, proxy services, personal hotspots or unauthorised browsers;
- install software, extensions or apps, or connect storage and hardware, without approval;
- damage, disrupt, probe or test systems without explicit authorisation;
- use school systems for fraud, gambling, political campaigning, commercial gain or unlawful activity;
- share passwords, verification codes or confidential links;
- upload school data to personal email, consumer cloud storage, social media or unapproved services;
- use another person's image, work or personal information without a lawful and appropriate basis;
- make recordings in school without permission.

8. Generative artificial intelligence

Generative AI may be used only where it is approved, age-appropriate, educationally justified and consistent with safeguarding, data-protection, equality, intellectual-property and procurement requirements.

- Only school-approved AI tools and accounts may be used for school work.
- Pupils must use AI only when a member of staff has explicitly permitted and supervised its use.
- Age restrictions and supplier terms must be checked before pupil access is enabled.

- Personal data, special-category data, safeguarding records, confidential material, photographs, identifiable pupil work or unpublished assessment information must not be entered into an AI system unless specifically authorised following advice from the DPO and DSL.
- Where authorised personal data is processed, the school must establish a lawful basis, transparency, retention and security arrangements and ensure the information is not used to train a public model.
- Outputs must be checked for accuracy, bias, fabricated information, inappropriate material and copyright concerns. AI output must never be relied upon as the sole basis for a safeguarding, disciplinary, admissions, SEND, assessment or other significant decision about a person.
- Users must acknowledge material AI assistance where required by the school or assessment rules and must not present AI-generated work dishonestly as wholly their own.
- Users must not use AI to create impersonations, deepfakes, bullying material, sexual content, malicious code, misinformation or content intended to evade safeguarding controls.
- The introduction of a new AI tool will trigger an appropriate risk assessment and, where required, a data protection impact assessment and filtering/monitoring review.

9. Data protection and confidentiality

- Personal information will be processed lawfully, fairly, transparently, securely and only for specified purposes.
- Users will access only the information required for their role and will not disclose it without authority.
- Consent will not be treated as the only lawful basis. Safeguarding information may be shared without consent where lawful and necessary to protect a child.
- Confidential information must use approved storage and transfer methods, appropriate access controls and encryption where required.
- Personal data breaches, misdirected emails, unauthorised access and lost devices must be reported immediately under the school's breach procedure; users must not attempt to conceal or investigate incidents independently.
- Data will be retained and securely deleted in accordance with the school's retention schedule.
- Privacy notices will explain relevant monitoring and the use of approved EdTech or AI services. Data-protection concerns and complaints will follow the school's accessible complaints process.

10. Email, cloud services and communication

- School business must be conducted through approved school accounts and platforms.
- Staff must check recipients carefully, use blind copy where appropriate, minimise personal data and apply secure transfer methods for sensitive information.
- Suspicious links, unexpected attachments, requests for passwords or payments and changes to bank details must be independently verified and reported.
- Auto-forwarding school email to personal accounts is prohibited unless specifically approved.
- Pupils may use school email and collaboration tools only under age-appropriate controls and supervision.
- Deleting an email does not necessarily remove it from backups, archives, audit logs or legal disclosure obligations.

11. Mobile, smart and personal devices

The school's separate Mobile Phone Policy determines when pupils may bring devices to school and how they are stored. For primary-aged pupils, personal mobile and smart devices must normally be switched off and stored in accordance with school procedures.

- Smartwatches, wearable cameras and other connected devices are covered in the same way as mobile phones.
- Personal hotspots, tethering and unauthorised connections must not be used to bypass school filtering.
- Staff must keep personal devices secure and must not use them to photograph, film or store information about pupils unless an exceptional, authorised procedure applies.
- School devices taken off-site remain subject to this policy, security controls and appropriate filtering and monitoring.
- Lost, stolen or compromised devices must be reported immediately.

12. Images, video and livestreaming

- Images and recordings will be created, stored and shared only for an authorised purpose and in accordance with the school's privacy information and consent arrangements.
- Staff will use approved school equipment and storage wherever pupils are identifiable.
- Livestreams and video calls must use approved platforms, appropriate privacy settings and professional backgrounds and conduct.
- Users must not record or distribute lessons, meetings, calls or other people without permission.
- Any concern involving sexual images, voyeurism, coercion, deepfakes or image-based abuse must be passed immediately to the DSL and handled as a safeguarding matter.

13. Social media and professional boundaries

- Staff must not communicate with pupils through personal social-media, messaging, gaming or email accounts.
- School communication with pupils and families will use approved channels.
- Staff must maintain professional boundaries and must not post confidential information, pupil images or content that could bring the school or their professional role into disrepute.
- Privacy settings do not guarantee confidentiality. Staff should assume that online content may be copied and shared.
- Safeguarding concerns discovered through social media must be reported to the DSL; staff should not conduct their own investigation.

14. Cyber security

- Accounts must use strong, unique passwords or passphrases and multi-factor authentication where available or required. Passwords must be changed if compromise is suspected or instructed by IT support.
- Users must never approve an unexpected authentication request or disclose a password or verification code.
- Devices must be locked when unattended, updated promptly and protected by approved anti-malware and firewall controls.
- Only authorised software, applications, extensions and removable media may be used.
- Phishing, malware, ransomware, unusual device behaviour, unauthorised access and suspected data loss must be reported immediately and the affected device disconnected only as directed by the incident procedure.
- The school will maintain appropriate backups, access controls, asset records, incident plans and recovery arrangements.

15. Online safeguarding concerns

The school recognises online safeguarding through the four areas of risk: content, contact, conduct and commerce. Concerns may arise on school systems or away from school and may involve child-on-child abuse, adults, strangers, organised groups or automated systems.

- Pupils should stop, preserve relevant evidence where safe, avoid forwarding harmful material and tell a trusted adult immediately.
- Staff must report concerns promptly to the DSL or deputy using the school's safeguarding system. Immediate danger or suspected crime will be escalated under safeguarding procedures.
- All incidents involving the making or sharing of nude or semi-nude images require a safeguarding response, whether described as consensual or non-consensual.
- Staff must not view, copy, print or forward sexual imagery of a child. Devices should be secured and advice sought from the DSL.
- Concerns about a member of staff, contractor or volunteer must be reported under the allegations and low-level-concerns procedures, including referral to the Headteacher, Chair of Governors or LADO as appropriate.

16. Incident response and sanctions

- Safeguarding and welfare take priority. The DSL will determine the safeguarding response and whether external agencies or the police should be involved.
- The school will record the concern, decisions, rationale, action and outcome.
- Technical evidence will be preserved lawfully; staff and pupils must not conduct unauthorised searches or investigations.
- Parents and carers will normally be informed unless doing so could increase risk or prejudice safeguarding or law-enforcement action.
- Responses will be proportionate, consistent and sensitive to age, intent, impact, SEND and vulnerability.
- Possible action includes education, restorative work, restriction or removal of access, action under the Behaviour Policy, staff disciplinary procedures, contract action, referral to external agencies or police, and recovery of loss where appropriate.
- Accidental access reported promptly and honestly will be treated differently from deliberate, repeated or concealed misuse.

17. Equality, SEND and accessibility

The school will apply this policy consistently and without unlawful discrimination. Reasonable adjustments, additional teaching and accessible reporting routes will be provided where needed. Decisions about filtering, monitoring and sanctions will consider age, developmental stage, SEND, language, vulnerability and the risk of disproportionate impact, while maintaining safeguarding and security.

18. Monitoring, review and record keeping

- The policy will be reviewed annually and after a serious incident, safeguarding review, material legal or guidance change, new technology, significant system change or identified weakness.
- Review will include feedback and evidence from safeguarding, IT, curriculum, behaviour, data protection and incident records.
- The Governing Body will receive appropriate assurance without being given unnecessary personal or sensitive information.

- The current policy and relevant AUP agreements will be communicated to pupils, parents, staff, governors, volunteers, visitors and contractors as appropriate.
- Acknowledgements, training records, filtering checks, monitoring actions and policy approvals will be retained in accordance with the school's retention arrangements.

Appendix A — Staff Acceptable Use Agreement

This agreement applies to employees, governors, volunteers, supply and agency staff and others given a school account or device. By signing, I confirm that I have read and will follow the Online Safety and Acceptable Use Policy.

- I will use school technology and information only for authorised professional purposes and limited approved personal use.
- I will use my own account, protect passwords and MFA codes, and lock devices when unattended.
- I will use approved accounts, applications, cloud storage and communication channels.
- I will not place personal, safeguarding or confidential data into an unapproved AI tool or online service.
- I will fact-check AI output, identify its use where required and retain professional responsibility for all work and decisions.
- I will maintain professional boundaries and will not contact pupils through personal accounts.
- I will use school equipment and approved storage for pupil images and recordings.
- I will not bypass security, filtering or monitoring, including through VPNs, hotspots or unauthorised software.
- I understand that authorised activity may be logged, filtered and monitored for safeguarding, security and operational purposes.
- I will immediately report safeguarding concerns to the DSL and cyber or data incidents through the school's procedures.
- I understand that misuse may lead to restriction of access, disciplinary action, referral to safeguarding authorities or police, or other appropriate action.

Name	
Role	
Signature	
Date	

Appendix B — Key Stage 2 Pupil Acceptable Use Agreement

I want to be a safe, kind and responsible digital citizen. I agree that:

- I will use school devices, accounts and internet access only when a trusted adult allows me.
- I will keep my password private and use only my own account.
- I will be kind and respectful. I will not bully, threaten, embarrass or pretend to be someone else.
- I will not share my address, phone number, password, location, private photographs or other personal information.
- I will not take or share photographs, video or audio without permission.
- I will not try to get around school filtering or use a VPN, proxy, personal hotspot or unauthorised app.
- I will use AI only when a teacher says I may. I will not enter anyone's personal information and I will say when AI has helped me if asked.
- I will think carefully about whether online information is true and will check with trusted sources.
- If I see something worrying, upsetting or inappropriate, I will stop and tell a trusted adult. I will not forward it to other pupils.
- If someone asks me to keep an online secret, meet them, send an image or do something uncomfortable, I will tell a trusted adult.
- I understand that the school may check and monitor use of its devices, accounts and network to help keep everyone safe.
- I understand that if I break these rules the school will help me understand what went wrong and may restrict my access or take action under the Behaviour Policy.

Pupil name	
Class	
Pupil signature	
Parent/carer signature	
Date	

Appendix C — EYFS and Key Stage 1 Pupil Agreement

These rules should be discussed with children in age-appropriate language.

- I ask before I use a device.
- I use my own login and keep my password private.
- I am kind when I use technology.
- I ask before taking a photograph or video.
- I do not share personal information.
- If something worries or upsets me, I stop and tell a trusted adult.
- I only use websites, apps and AI tools that my teacher has chosen.
- I look after school equipment.

Pupil name	
Class	
Discussed with	
Parent/carer signature	
Date	

Appendix D — Visitors, Volunteers and Contractors

Anyone given access to school technology or information must:

- use only the access and equipment authorised for their visit or work;
- keep credentials secure and use identifiable accounts where provided;
- maintain confidentiality and comply with safeguarding and data-protection requirements;
- not photograph, record or contact pupils unless expressly authorised and supervised;
- not bypass filtering, monitoring or security or connect unauthorised equipment;
- report harmful content, safeguarding concerns, cyber incidents and data breaches immediately to their school contact;
- understand that authorised use may be logged and monitored and that access may be withdrawn.

Name / organisation	
Purpose of access	
School contact	
Signature	
Date	

Authoritative references

- **Keeping Children Safe in Education 2026:** https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- **DfE filtering and monitoring core standard:** https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard
- **DfE cyber security core standard:** https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard
- **DfE generative AI in education:** https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education
- **DfE data protection in schools:** https://www.gov.uk/guidance/data-protection-in-schools
- **Prevent Duty Guidance:** https://www.gov.uk/government/publications/prevent-duty-guidance