

Online Safety Policy

St Matthew's Catholic Primary School



Love, Learn and Shine together with Jesus

Safeguarding children in a connected world 2026 to 2027

Approved by	Governing Body
Policy owner	Headteacher and Designated Safeguarding Lead
Approval date	September 2026
Review date	September 2027, or sooner if guidance or practice changes

1 Policy statement

Online safety is an integral part of safeguarding at St Matthew's Catholic Primary School. The school will protect and educate pupils, equip staff to identify and respond to harm, and maintain appropriate technical safeguards. This policy applies to school technology and to online activity outside school where it affects the safety, wellbeing or education of a pupil or the school community.

The school recognises the four areas of online risk identified in Keeping Children Safe in Education: content, contact, conduct and commerce. Risks include harmful or illegal material; grooming and exploitation; bullying and sexual harassment; misinformation; radicalisation; self-harm and suicide content; scams; generative-AI chatbots; and the creation or sharing of explicit or manipulated images.

2 Aims

- provide a safe digital environment while supporting purposeful teaching and learning;
- teach pupils the knowledge and confidence to make safe, respectful and informed choices;
- identify pupils who may be more vulnerable online and provide appropriate support;
- ensure concerns are recognised, reported, recorded and acted upon promptly;
- maintain effective filtering, monitoring, cyber security and data-protection arrangements; and
- work with parents, governors, the local authority, police and specialist agencies where necessary.

3 Roles and accountability

Role	Main responsibilities
Governing Body	Ensures appropriate policies, training, filtering and monitoring are in place; reviews assurance and challenge at least annually.
Headteacher	Ensures implementation, resources, staff conduct, incident management and communication with families and agencies.
DSL	Holds lead responsibility for online safeguarding and understanding the filtering and monitoring systems; reviews reports and ensures concerns are acted upon.
Safeguarding team	Receives NfGL alerts, checks them against the device/IP information where needed, records safeguarding concerns on CPOMS and escalates promptly.
DPO – Mrs Louisa Chamberlain	Advises on lawful processing, privacy, data-sharing, images, AI and personal-data breaches.
IT support	Maintains secure systems and filtering/monitoring; documents changes; supports checks, reviews and incident response.
Teaching staff	Teach online safety, supervise use, model safe practice and report concerns without delay.
All staff and volunteers	Follow policy and training, maintain professional boundaries and report any concern to the DSL.
Pupils	Follow the pupil agreement, behave respectfully and seek help when worried.
Parents and carers	Support school expectations, supervise age-appropriate use and report concerns affecting a child or the school community.

4 Education and prevention

Online safety is taught through computing, relationships and health education, safeguarding work, assemblies and age-appropriate discussion across the curriculum. Teaching will be inclusive and adapted for age, development, SEND, EAL and known vulnerabilities.

- privacy, passwords, personal information, consent and digital footprints;
- respectful communication, cyberbullying, discrimination and how to report;
- healthy technology use, persuasive design, gaming, gambling and in-app purchasing;
- grooming, exploitation, coercion, sextortion and unsafe contact;
- nude and semi-nude images, sexual harassment, manipulated images and deepfakes;
- misinformation, disinformation, scams, phishing and evaluation of sources;
- copyright, ownership, plagiarism and responsible use of generative AI; and
- how to block, report, preserve evidence safely and seek help.

Staff receive online-safety and filtering-and-monitoring information at induction and through regular safeguarding updates. Parents are supported through communications, the website and workshops or signposting where appropriate.

5 Reporting and responding to concerns

A pupil may report to any trusted adult. Staff must listen, reassure the child that they have done the right thing, avoid blame, establish only the information needed for immediate safety and report to the DSL without delay. Safeguarding concerns and actions will be recorded on CPOMS. Urgent risk is escalated immediately to the Headteacher/DSL and emergency services where required.

Staff must not promise confidentiality, conduct their own investigation, contact an alleged perpetrator, or ask a child to download, forward or repeatedly describe illegal imagery. Devices should be secured and potential evidence preserved without unnecessary viewing. The DSL will follow KCSIE, the school Child Protection and Safeguarding Policy and relevant national guidance, including consultation or referral to children's social care, the police, CEOP, the Internet Watch Foundation, the LADO or Prevent partners as appropriate.

6 Child-on-child abuse and harmful sexual behaviour

Online child-on-child abuse may include bullying, harassment, coercion, sexual comments, sharing nude or semi-nude images, upskirting, sexualised deepfakes, impersonation, exclusion, threats or abuse in group chats, games or social media. The school will never dismiss this as banter or an inevitable part of growing up.

Each case will be assessed individually. The school will consider the wishes and safety of the child harmed, the age and development of all children, SEND and vulnerability, power imbalance, recurrence, coercion and whether a crime may have occurred. Separate support and proportionate safety plans will be considered for the child harmed, the child alleged to have caused harm and other affected pupils. Behaviour sanctions may apply alongside safeguarding support.

7 Nude and semi-nude images and deepfakes

Creating, possessing or sharing sexual imagery of a child, including AI-generated or manipulated imagery, may be a criminal and safeguarding matter. Staff who become aware of such imagery must report immediately to the DSL. Other than in the exceptional circumstances permitted by national guidance for the DSL, staff must not view, copy, print, save, forward, delete or ask a pupil to share the image. The DSL will use the UKCIS guidance, undertake a risk assessment and decide whether police or children's social care involvement is required.

8 Filtering and monitoring

The school uses NfGL filtering and monitoring. Filtering restricts access to illegal and harmful material; monitoring helps identify concerning searches, language or activity. Safeguarding-team members receive daily alerts that can be checked against the IP address and device information. Alerts are triaged according to risk, and any safeguarding concern is followed up and recorded on CPOMS.

- The DSL leads on safeguarding and online safety and understands the systems and escalation routes.
- A designated senior leader, the DSL and IT support review the effectiveness of filtering and monitoring at least annually.
- Operational checks take place regularly and after significant system, network or safeguarding changes. Checks and decisions about what is blocked or allowed are recorded.

- IT support maintains the system and reports failures. Staff report over-blocking, under-blocking, concerning activity and any suspected failure immediately.
- Filtering and monitoring are applied proportionately to school-managed devices and services, including consideration of generative AI. They do not replace active adult supervision.
- Monitoring is not guaranteed to be continuous outside school hours. The school communicates this limitation and provides routes for urgent reporting.

9 Generative artificial intelligence

The school has a separate AI Policy. Only school-approved tools may be used. Staff may use the school-approved Google Gemini platform and Chalkie AI for appropriate teaching and planning purposes. Any pupil-facing use must meet age restrictions, be risk assessed, supervised and use a product with appropriate safety, privacy, filtering and monitoring features.

- No pupil photograph, voice recording, name, identifiable work, safeguarding information, medical information, SEND record, staff personal data or confidential school information may be entered or uploaded.
- AI output must be checked by a competent adult for accuracy, bias, suitability, copyright and safeguarding risk.
- AI must not replace professional judgement or make final decisions about pupils or staff.
- Deepfakes, impersonation, fabricated evidence, sexualised images and harmful chatbot interactions are prohibited and will be managed as safeguarding concerns.
- Pupils are taught that AI output may be inaccurate, biased or manipulative and that responsible use includes acknowledging assistance where appropriate.

10 Images, video and audio

Staff may record pupils only on authorised school devices, for an agreed purpose and in accordance with consent choices and the Safe Use of Children's Photographs Policy. Personal devices must never be used. Files must be stored in approved school systems and deleted when no longer required under the retention schedule.

Because publicly available images may be copied or manipulated using AI, the school will normally use partial, group, distant, activity-focused or rear-view images for external publication and avoid high-resolution full-face images. Images will not normally be linked to a child's full name or other identifying information. Identifiable pupil images must never be uploaded to generative-AI tools.

11 Mobile phones, wearable and recording technology

Pupils must not use phones, smartwatches or other connected or recording devices during the school day unless the school has approved a specific medical or SEND arrangement. Only Year 6 independent walkers with written permission may bring a phone; it must be handed in on arrival and collected at the end of the day. Secret photography, recording, livestreaming or location sharing is prohibited.

Staff devices must be silent and stored away while working with pupils and may be used only in designated areas or for an authorised emergency. Visitors and contractors must not photograph, film or record pupils. Any necessary recording of buildings or equipment must be authorised and supervised.

12 Social media and communication

School communication with pupils and families takes place through approved channels. Staff must maintain professional boundaries and must not use personal accounts, numbers or messaging services to communicate with pupils. Staff must not discuss confidential school matters, post images of pupils or make comments that could bring the school into disrepute.

Online incidents outside school may be addressed where they create a safeguarding risk, target a member of the school community, disrupt education or damage relationships. The school may ask that content is preserved, removed or reported and may involve parents, platforms, the local authority or police.

13 Data protection and cyber security

Personal information is processed in accordance with UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, school privacy notices and the Data Protection Policy. Suspected loss, disclosure, unauthorised access or cyberattack must be reported immediately to the DPO and authorised IT support. Safeguarding concerns must also be reported to the DSL.

- strong unique passwords and multifactor authentication where available;
- least-privilege access, prompt account removal and secure device configuration;
- security updates, antivirus, backups, encryption and tested recovery arrangements;
- phishing awareness and independent verification of financial or account changes; and
- secure disposal and retention of devices and information.

14 Vulnerable pupils and reasonable support

Some pupils may face additional online risk because of age, SEND, communication needs, EAL, care experience, mental health, family circumstances or previous abuse. The school will work with the child and family, adapt teaching and supervision, and may apply individual filtering, monitoring, device or safety arrangements where proportionate. Support will avoid blame and unnecessary restriction while prioritising safety.

15 Incidents, sanctions and records

Responses will be safeguarding-led, proportionate and consistent. The school may restrict access, secure a device, preserve evidence, contact parents and agencies, provide education or pastoral support, and apply the Behaviour or Staff Disciplinary Policy. Decisions, advice, referrals and outcomes will be recorded on CPOMS or the appropriate confidential staff, data-protection or technical record.

16 Monitoring, assurance and review

- annual review of the school's overall online-safety approach and filtering/monitoring provision;
- regular review of CPOMS themes, NfGL alerts, behaviour incidents, bullying, complaints, pupil voice and curriculum evidence;
- governor scrutiny of training, incident themes, filtering/monitoring assurance and actions, without unnecessary personal information;
- review following a serious incident, technology change or new legal or safeguarding guidance; and
- annual issue and review of age-appropriate Acceptable Use Agreements.

17 Related school policies

- Child Protection and Safeguarding Policy
- Acceptable Use Policy and agreements
- AI Policy
- Data Protection Policy and privacy notices
- Staff Code of Conduct
- Behaviour and Anti-Bullying Policies
- Mobile Phone Policy
- Safe Use of Children's Photographs Policy
- RSHE Policy
- Whistleblowing, complaints and disciplinary procedures
- Business continuity and cyber incident arrangements

Key legislation and guidance

This policy should be read alongside the school's Child Protection and Safeguarding Policy and the related school policies listed below. It has regard to:

- Keeping Children Safe in Education 2026 (statutory guidance).

- Education Act 2002, including the duty to safeguard and promote pupils' welfare.
- Children Act 1989 and Children Act 2004.
- Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025.
- Equality Act 2010 and Human Rights Act 1998.
- Prevent duty guidance and statutory Relationships Education, Relationships and Sex Education and Health Education guidance.
- DfE Filtering and Monitoring Core Standard and Cyber Security Core Standard.
- DfE Generative Artificial Intelligence in Education and Generative AI Product Safety Standards.
- UKCIS Sharing Nudes and Semi-Nudes guidance and DfE Searching, Screening and Confiscation advice.
- DfE Mobile Phones in Schools guidance.