



Whole School Social Media Policy

Love Learn and Shine together with Jesus

Policy owner	Headteacher Mrs Claire Sime
Approved by	Governing Board
Reviewed	September 2026
Next review	September 2027 or sooner if guidance changes
Applies to	Staff governors volunteers pupils parents carers visitors and contractors

Purpose

St Matthew's Catholic Primary School values safe, positive and respectful online communication. This whole-school policy sets clear social media expectations for staff, governors, volunteers, pupils, parents, carers, visitors and contractors. It protects children's welfare and privacy, maintains professional boundaries, supports staff wellbeing and provides clear, proportionate routes for responding to concerns.

The policy must be read with the Staff Code of Conduct, Staff Acceptable Use Policy, Parent Carer and Visitor Code of Conduct, Complaints Policy, Safeguarding and Child Protection Policy, Online Safety Policy, Relationships and Behaviour Policy, Data Protection Policy and relevant disciplinary or capability procedures. Where documents overlap, the requirement offering the strongest lawful safeguarding protection will apply.

Scope

This policy applies to school-related use and to public or private online activity with a sufficient connection to the school, its pupils, families, staff, governors, volunteers, contractors, activities, operations or reputation. It includes:

- WhatsApp and other messaging groups, including year-group and class groups;
- Facebook, Instagram, TikTok, X, Snapchat, YouTube, online forums and community pages;
- email, text messages, direct messages, blogs, livestreams, gaming chat and emerging platforms; and
- posts, comments, reactions, reviews, photographs, video, audio, screenshots, forwarded messages and altered or AI-generated content.

The policy applies whether an account uses a real name, nickname, anonymous identity or another person's account, and whether content is original, reposted, forwarded, liked or otherwise amplified.

Principles

The school recognises the rights of members of its community to a private life, lawful expression, appropriate professional discussion and legitimate criticism or complaint. This policy does not prohibit fair, lawful criticism, protected whistleblowing, trade-union activity or reporting a concern to a person or body entitled to receive it.

That right must be exercised responsibly. Freedom to express a view does not justify threats, harassment, discrimination, bullying, the disclosure of confidential or safeguarding information, or communications that may be otherwise unlawful. A private group should not be treated as confidential: messages and screenshots can be copied, forwarded and shared with the school or others.

Children learn from adult behaviour. Parents, carers and visitors are expected to model the same kindness, accuracy, restraint and respect online that the school expects in person.

Responsibilities

The governing board has strategic oversight of online safety, filtering and monitoring and the effectiveness of this policy. The Headteacher is responsible for implementation and staff conduct. The Designated Safeguarding Lead leads on safeguarding and online-safety concerns. All users must report concerns promptly and cooperate with proportionate enquiries.

Staff governors volunteers and contractors

This section applies to employees, agency staff, governors, volunteers, students on placement and contractors where they have access to pupils, information, systems or the school community. It supplements the Staff Code of Conduct and does not replace employment, safeguarding, whistleblowing or disciplinary procedures.

Professional boundaries and communication

- use only school-approved accounts, systems and contact details for communication with pupils and for routine communication with parents or carers;

- never accept or initiate friend, follow, direct-message, group-chat, gaming or similar contact with a current pupil through a personal account;
- do not establish personal online contact with a former pupil who is under 18. Any exceptional pre-existing family or community connection must be declared to the Headteacher or Designated Safeguarding Lead and managed transparently;
- do not use disappearing-message functions, personal livestreams or private social media accounts for teaching, pastoral support or school business;
- keep communication transparent, necessary, professional and capable of appropriate oversight; and
- report immediately to the Designated Safeguarding Lead any accidental contact, inappropriate message, boundary concern, suspected grooming, sexual content or attempt by a pupil to move communication onto a personal channel.

Staff must not rely on a disclaimer such as “views are my own” to excuse conduct that breaches professional standards, confidentiality, safeguarding duties or this policy. Personal accounts should not be presented as official school accounts.

Personal social media use

- apply privacy settings carefully while recognising that no setting guarantees confidentiality and content may be copied or shared;
- avoid identifying their employer on personal profiles where this is unnecessary, and never imply that personal views are those of the school;
- not post about pupils, individual families, confidential school matters, safeguarding cases, complaints, staffing matters or internal deliberations;
- not post content that could reasonably call into question their suitability to work with children, compromise professional boundaries, seriously damage trust or breach the Staff Code of Conduct;
- not make discriminatory, threatening, harassing, bullying or seriously offensive posts or engage in online conduct incompatible with their professional role;
- not use school logos, branding, photographs, recordings or school-created material on a personal account without authorisation;
- not discuss colleagues or workplace disputes online in a manner that breaches confidentiality, dignity-at-work expectations or lawful management instructions; and
- consider whether liking, reposting, tagging or joining a group may communicate endorsement or increase the reach of harmful material.

Images information and school accounts

- publish pupil images, names or work through authorised school accounts only, in accordance with the school's lawful basis, privacy information and consent arrangements where consent is relied upon;
- store and transfer school information only through approved systems and devices and never upload personal data or school content to an unapproved service;
- obtain authorisation before creating an account, page, channel or group in the school's name;
- use strong authentication, protect access credentials and transfer control of official accounts when roles change; and
- report mistaken posts, account compromise, data loss or suspected data breaches immediately so that content can be contained and the Data Protection Officer informed where required.

Concerns about staff conduct

A social media concern about an adult working in or on behalf of the school must be reported to the Headteacher. A concern about the Headteacher must be reported to the Chair of Governors. Safeguarding allegations and low-level concerns will be managed under Keeping Children Safe in Education 2026 and the school's safeguarding procedures. Staff must not investigate such concerns through social media or alert the person concerned where this could prejudice safeguarding action.

A breach may be considered under the Staff Code of Conduct, safeguarding, data-protection, whistleblowing, grievance, capability or disciplinary procedures as appropriate. Action will not be automatic: the school will consider the facts, context, seriousness, impact, role, professional obligations

and employment rights, and will follow the applicable fair procedure. Serious misconduct may amount to gross misconduct, but that determination can be made only under the relevant procedure.

Pupils

Pupils are taught to use technology safely, respectfully, responsibly and with age-appropriate understanding. They must follow the Pupil Acceptable Use Agreement, Relationships and Behaviour Policy, Online Safety Policy and staff instructions.

- use only approved accounts and platforms for school learning and keep passwords secure;
- communicate respectfully and never bully, threaten, harass, discriminate against, impersonate or deliberately humiliate another person;
- not create or share sexual, violent, hateful, extremist, illegal or age-inappropriate content;
- not photograph, record, livestream or share images of pupils or staff in school without permission;
- not share another person's personal information, location, private messages or images without a proper reason and permission;
- not create anonymous accounts, fake profiles, altered images, deepfakes or rumours to target another person or mislead others; and
- tell a trusted adult immediately about threats, coercion, grooming, sexual images, harmful content, bullying, account compromise or anything online that makes them feel unsafe.

The school may address online behaviour that occurs away from school where the law and school policy allow and there is an effect on pupils, staff, school discipline, safeguarding, welfare or the orderly running of the school. Responses will be educational and proportionate, taking account of age, SEND, vulnerability, context and the school's behaviour and safeguarding duties. Safeguarding action may be required whether or not a sanction is imposed.

Expected online conduct for parents carers and visitors

Parents, carers and visitors should:

- pause and check the facts before posting, forwarding or commenting;
- raise school concerns directly with the appropriate member of staff and use the Complaints Policy where needed;
- disagree with ideas or decisions without attacking, humiliating or targeting individuals;
- protect the identity, dignity and welfare of children and families;
- follow any school instructions about photography, filming, recording and posting at school events;
- use official school contact routes rather than personal social media accounts to contact staff;
- correct or remove inaccurate or inappropriate content promptly when a concern is identified; and
- report online content that creates an immediate safeguarding or safety concern.

Content and conduct that are not acceptable

The following conduct is not acceptable where it concerns or affects the school community. The examples are not exhaustive.

Abuse intimidation and targeted behaviour

- threatening, menacing, abusive, humiliating, discriminatory or seriously offensive content;
- harassment, stalking, cyberbullying, repeated unwanted contact or encouraging others to target an individual;
- personal attacks, name-calling, swearing directed at another person or comments intended to cause fear or serious distress;
- creating or joining an online campaign against an identifiable child, family, employee, governor or volunteer; and
- sharing a person's contact details, location or other private information to expose them to contact, intimidation or harm.

Allegations rumours and misleading content

- presenting rumour, assumption or one account of an incident as established fact;

- publishing an allegation about a child or adult instead of reporting it through the appropriate school, safeguarding or complaints route;
- knowingly posting or forwarding false information, or continuing to circulate information after becoming aware that it may be inaccurate; and
- editing, cropping, miscaptioning or generating content in a way that creates a materially misleading impression.

Privacy safeguarding and recordings

- identifying or discussing another person's child, special educational need, disability, medical need, behaviour, safeguarding history or family circumstances;
- sharing confidential school correspondence, reports, meeting notes, screenshots or personal information without a proper reason or lawful basis;
- posting images, video or audio of other children or adults contrary to school event rules or in a way that creates a privacy, welfare or safeguarding risk;
- livestreaming from school premises or recording lessons, meetings or conversations without the school's knowledge; and
- contacting pupils through personal accounts or encouraging a child to share confidential or inappropriate material.

Taking a photograph for personal or household use is not automatically a breach of data protection law. However, the school may prohibit or limit photography and recording on its premises or at events for safeguarding, privacy or operational reasons. Wider publication may engage different legal and platform rules. Parents and visitors must always follow the instructions given for the particular event.

Identity intellectual property and security

- impersonating the school, a member of staff, a pupil, governor or another parent;
- creating an account, page or group that could reasonably appear to be an official school account;
- using the school name, crest or logo in a way that falsely suggests authorisation, endorsement or official status;
- disclosing security arrangements, access codes, staff or pupil locations, or information that could compromise safety; and
- posting, requesting or sharing illegal content, hate material, terrorist content or material that promotes serious harm.

Parent WhatsApp and messaging groups

Parent-run groups are independent of the school. The school does not administer or monitor them and is not responsible for their membership or content. They can be useful for general reminders and mutual support, but they must not be used as an alternative complaints process or to investigate incidents involving children.

Group administrators are encouraged to publish clear rules, remove content that breaches those rules and direct school concerns to the school. Members should not assume that messages will remain within the group. Where messages or screenshots are lawfully shared with the school, the school may consider them if they raise a safeguarding, welfare, safety, staff wellbeing or serious conduct concern.

No parent or administrator should pressure another person to disclose private messages, remain in a group, take sides or participate in a campaign. Parents should leave a group, mute it, report content or seek support if participation is causing distress or conflict.

Raising concerns and complaints

1. Contact the class teacher where the concern relates to ordinary classroom matters.
2. Contact the school office where the correct person is unclear or a senior leader is required.
3. Report safeguarding concerns promptly to the Designated Safeguarding Lead. Contact the police or children's social care directly where appropriate; call 999 if someone is in immediate danger.
4. Use the published Complaints Policy if an informal concern is not resolved or a formal response is required.

Posting about a complaint does not pause, replace or accelerate the school's complaints procedure. The school will protect confidential information and may be unable to respond publicly to a claim even where the account presented online is incomplete or inaccurate.

Reporting online concerns to the school

A report should, where possible, include the platform or group, date and time, username, link and an unedited screenshot showing enough context to understand the communication. The person reporting should not provoke further exchanges or circulate the material more widely than necessary. Content involving a child should be handled particularly carefully.

The school will consider whether the matter falls within its role and policies. It will not investigate every disagreement between adults or act as the moderator of independent parent groups. It may act where there is a sufficient connection to the school and the content affects safeguarding, safety, school operations, a child's education or welfare, staff wellbeing, or the rights and legitimate interests of members of the school community.

How the school may respond

The response will be proportionate to the content, context, audience, reach, repetition, impact, intent where it can reasonably be assessed, any previous incidents, safeguarding risk and relevant equality or accessibility needs. Except where urgent action is needed, the school will normally preserve the available evidence, establish the relevant facts and give the person concerned an opportunity to provide their account.

Possible response	What this may involve
Informal resolution	Discuss the concern; clarify facts and expectations; ask for content to be removed, corrected or no longer circulated.
Written action	Issue a reminder, warning or behaviour agreement and retain an appropriate record.
Communication arrangements	Nominate a single contact, require written communication, set reasonable response arrangements or manage abusive or unreasonably repetitive contact without removing access to the Complaints Policy.
Platform action	Report content or an account to the relevant social media, messaging, review or hosting service.
Safeguarding and support	Act under safeguarding procedures; seek help from the Local Authority, Archdiocese, Professionals Online Safety Helpline or another appropriate agency.
Site access	Apply the Parent Carer and Visitor Code of Conduct, including conditions on access or the fair process for a temporary or continuing site bar where online conduct indicates a risk to pupils or staff.
Police or legal advice	Contact the police in an emergency or where conduct may involve threats, violence, harassment, stalking, hate crime, malicious communications or another offence; seek legal advice on other serious matters.

The school may ask an individual to preserve content and stop further publication while a matter is assessed. Removing a post does not necessarily remove screenshots or undo its impact. The school cannot

compel a platform to remove content and cannot determine criminal liability, defamation or a data-protection breach; those decisions rest with the relevant authority or court.

Parents supporting children online

Parents and carers are expected to provide age-appropriate supervision, follow platform age requirements, discuss privacy and respectful conduct, and cooperate with the school when online behaviour affects pupils or learning. They should not ask children to obtain screenshots, question other pupils or intervene in a child-related dispute through social media. Harmful content should be preserved only as necessary for reporting and should not be repeatedly viewed or circulated.

Official school social media accounts

Only staff authorised by the Headteacher may create, administer or post to an official school account. Each account must have a clear educational or communication purpose, appropriate oversight, secure access and at least two authorised administrators where practicable. Content must be accurate, professional, accessible and consistent with safeguarding, copyright, data-protection and political-impartiality requirements.

Official accounts must not be used to discuss individual complaints, disclose confidential information, conduct private conversations with pupils or engage in arguments. Comments or messaging functions may be limited where moderation cannot be managed safely. Account access must be reviewed when staff roles change, and obsolete accounts must be securely transferred, archived or closed.

Safeguarding Prevent and equality

Content that suggests abuse, exploitation, grooming, self-harm, serious violence, radicalisation or another safeguarding risk will be referred to the Designated Safeguarding Lead and managed under safeguarding procedures. The school will have regard to its Prevent duty and will refer concerns through the appropriate safeguarding or police route.

Discriminatory abuse and harassment connected with race, religion or belief, sex, sexual orientation, gender reassignment, disability, age or another protected characteristic will be taken seriously. The school will also consider reasonable adjustments and communication needs before deciding how to respond.

Information handling

The school may retain proportionate records of reports, messages, screenshots, correspondence, decisions and actions in accordance with its data-protection and records-management responsibilities. Information will be shared only where there is a lawful reason, including safeguarding, safety, legal advice, responding to complaints, or the prevention or investigation of crime. A person sending evidence to the school should share only what is relevant and should avoid unnecessary disclosure of children's or third parties' personal information.

The school does not routinely monitor private personal accounts. It may review public material, activity on school systems or devices, or material lawfully supplied to it where there is a legitimate safeguarding, employment, educational, legal or operational reason. Any monitoring will be necessary, proportionate, transparent where appropriate, and carried out in accordance with school policies and applicable law. School filtering and monitoring systems apply to school networks and managed devices.

Legal and guidance framework

This policy has regard to the legal and guidance framework relevant to online conduct and the school's response, including:

- the Education Act 1996, including section 547, and Department for Education guidance on controlling access to school premises;
- the Education and Inspections Act 2006 and the school's statutory behaviour responsibilities;
- the Children Act 1989 and Children Act 2004 and current statutory safeguarding guidance;

- Keeping Children Safe in Education 2026, including allegations and low-level concerns about adults working with children;
- the Teachers' Standards and other applicable professional standards;
- the Equality Act 2010;
- the Protection from Harassment Act 1997;
- the Defamation Act 2013;
- the Online Safety Act 2023 and other applicable communications and public-order law;
- the UK General Data Protection Regulation and Data Protection Act 2018; and
- the Counter-Terrorism and Security Act 2015 and Prevent duty guidance.

References to legislation do not mean that every breach of this school policy is unlawful. Equally, conduct may be referred for advice even if the school cannot determine whether an offence or civil wrong has occurred.

Monitoring and review

The Headteacher is responsible for implementing this policy. The governing board will approve and review it. The policy may be reviewed earlier following a serious incident, a change to the Parent Carer and Visitor Code of Conduct, or a change in legislation or guidance.