



Social Media Policy

Safe, respectful and responsible communication online

Policy owner	Headteacher and Designated Safeguarding Lead
Responsible governor	Safeguarding Governor
Approved by	Local Governing Body
Policy date	September 2026
Next review	September 2027 or sooner if guidance changes
Applies to	Staff, governors, volunteers, pupils, parents and visitors

Our Mission

“We are proud of our school as a place of learning, prayer and happiness. Hand in hand with God, Our Lady and St. Joseph, we promise to work hard and be kind to one another so that we can grow stronger together in our faith.”

Our online communication will reflect our Catholic ethos through kindness, dignity, honesty and respect.

Statement of Intent

St Joseph's Catholic Voluntary Academy recognises that social media can strengthen communication, celebrate learning and build positive relationships with families and the wider community. It also creates safeguarding, reputational, privacy and information-security risks that must be managed carefully.

This policy establishes clear expectations for official school accounts and for the professional and personal use of social media by staff, governors and volunteers. It should be read alongside the school's Online Safety, Safeguarding and Child Protection, Staff Code of Conduct, Data Protection, Acceptable Use, Behaviour, Anti-Bullying, Complaints and Whistleblowing policies.

The school will use social media only where it supports education, communication or community engagement and can be managed safely, lawfully and professionally.

1 Aims

- protect pupils, staff and the school community from harm;
- communicate accurately and positively with parents, carers and the wider community;
- celebrate pupils' learning and the life of the school appropriately;
- promote responsible digital citizenship and online safety;
- protect personal data, confidentiality and intellectual property; and
- ensure concerns and incidents are reported and managed promptly.

2 Scope and Definitions

This policy applies to employees, agency and supply staff, governors, volunteers, contractors, pupils, parents and carers when their use of social media relates to the school or could reasonably affect the school community.

Social media includes social networks, messaging services, video-sharing platforms, blogs, forums, livestreaming services, collaborative platforms and any online service that allows users to create, publish, comment on or share content.

An official account is an account approved by the Headteacher, created for school business and controlled through school-authorised access arrangements. The current official channels will be listed on the school website or communicated directly by the school.

3 Legal and Statutory Framework

The school will act in accordance with relevant legislation and guidance, including:

- UK General Data Protection Regulation and the Data Protection Act 2018;
- Education Act 2002 safeguarding duties;
- Children Act 1989 and Children Act 2004;
- Equality Act 2010;
- Human Rights Act 1998;
- Copyright, Designs and Patents Act 1988;
- Online Safety Act 2023, where relevant to school activity; and
- the current Department for Education statutory guidance Keeping Children Safe in Education.

4 Roles and Responsibilities

4.1 Local Governing Body

The Local Governing Body approves this policy and monitors assurance that suitable safeguarding, data-protection and account-security controls are in place.

4.2 Headteacher

The Headteacher has overall responsibility for the school's social media activity, approves official accounts and authorised users, ensures concerns are investigated and may require content to be amended or removed.

4.3 Designated Safeguarding Lead

The Designated Safeguarding Lead advises on safeguarding risks, ensures disclosures and concerns are managed through safeguarding procedures and liaises with external agencies where required.

4.4 Data Protection Lead

The Data Protection Lead advises on lawful processing, privacy information, image use, retention, data breaches and data-subject rights.

4.5 Authorised Account Users

Authorised users must follow this policy, use secure school-approved access, check content carefully, protect credentials and report mistakes, unauthorised access or concerning interactions immediately.

5 Official School Accounts

- Only the Headteacher may approve the creation, closure or substantial change of an official account.
- Accounts must use the school's official name and branding and must not be created as personal profiles where an organisational account is available.
- At least two appropriate members of staff must have oversight of each account so that access and continuity do not depend on one person.
- Posts must be accurate, respectful, accessible and consistent with the school's Catholic ethos.
- Official accounts must not be used for confidential matters, complaints, safeguarding reports or urgent messages.
- Comments and direct messages will be moderated. Offensive, discriminatory, threatening, unlawful or safeguarding-related content may be hidden, removed, restricted or reported.
- The school may pause comments or posting where this is necessary to protect individuals or manage an incident.

6 Photographs, Video and Audio

Images, recordings and captions can reveal personal data. Staff must use professional judgement and the school's consent and data-protection arrangements before capturing or publishing content.

- Pupils must be told when photographs, video or audio are being captured and must be treated with dignity and respect.
- The current consent or objection record must be checked before publication.
- Names, name labels, addresses, timetables, location data and other identifying details must not be published unless specifically authorised and necessary.
- Content must not show pupils in an undignified, vulnerable or inappropriate context.
- The background of every image or recording must be checked for confidential or identifying information.
- School-owned devices must normally be used. Any exceptional use of a personal device requires prior Headteacher authorisation and immediate secure transfer and deletion.
- Images must not be edited or combined in a misleading or harmful way.

7 Posting and Moderation Standards

- School-related content must be published through official accounts by authorised users.
- Posts must not identify an individual pupil unnecessarily or disclose special-category, safeguarding, medical or SEND information.
- A second authorised person should check sensitive, unusual or high-profile posts before publication.
- Copyrighted material, music, photographs, artwork or logos must be used only with appropriate permission or licence.
- Livestreaming requires a specific risk assessment and prior approval from the Headteacher and DSL.
- Mistakes must be corrected promptly and, where personal data may have been exposed, reported immediately under the data-breach procedure.

8 Staff, Governors and Volunteers

The same professional standards apply online as offline. Privacy settings reduce visibility but do not make content private.

- Personal accounts must not be used to communicate with current pupils about school matters.

- Staff must not accept or initiate social-media connections with current pupils through personal accounts.
- Staff should maintain appropriate professional boundaries with parents and carers and use approved school channels for school business.
- Confidential information, internal discussions, complaints, pupil information and images obtained through work must never be posted on personal accounts.
- Staff must not present personal opinions as the views of the school or use the school's branding in a misleading way.
- Content that is discriminatory, harassing, defamatory, threatening, unlawful or likely to undermine safeguarding or professional trust is prohibited.
- Concerns about colleagues must be raised through the appropriate safeguarding, whistleblowing, grievance or complaints route, not on social media.

9 Parents, Carers and Visitors

Parents, carers and visitors are encouraged to engage positively with official school content. They must respect the privacy and dignity of pupils, staff and other families.

- Photographs or recordings taken at school events must not be published if the school has restricted photography or if doing so would identify another child without appropriate permission.
- Children or other families must not be tagged or identified in school content without permission.
- Complaints, safeguarding concerns and personal matters should be raised directly with the school through the published procedures rather than through public comments.
- Abusive, discriminatory, threatening, defamatory or otherwise inappropriate content may be removed and the account restricted or reported.

10 Pupils

Pupils are taught to use technology safely, respectfully and responsibly. The school does not encourage pupils to create accounts below a platform's minimum age and expects families to follow platform terms and age requirements.

- Pupils must not impersonate the school, a member of staff or another pupil.
- Pupils must not tag or identify other pupils in school photographs without permission.
- Bullying, harassment, discrimination, threats and sharing private information are prohibited and will be addressed through school procedures.
- Pupils should save evidence and tell a trusted adult if something online makes them feel worried, unsafe or pressured.

11 Passwords and Account Security

- Each authorised user must use an individual school-controlled login where the platform allows it; shared credentials must be avoided.
- Strong, unique passwords and multi-factor authentication must be used wherever available.
- Passwords, recovery codes and authentication prompts must not be shared or approved unexpectedly.
- Access must be reviewed at least termly and removed immediately when a person's role changes or employment ends.
- School accounts must not use a personal email address or personal telephone number for recovery where an organisational option is available.
- Suspected compromise, phishing, accidental publication or unauthorised access must be reported immediately.

12 Incidents, Safeguarding and Data Breaches

Any social-media activity that raises a concern about a child must be reported to the DSL immediately and recorded in accordance with safeguarding procedures. Staff must not investigate by contacting a pupil through a personal account.

Threats, hate incidents, impersonation, harassment, criminal content or persistent abuse may be reported to the platform, the Trust, the local authority, the police or other relevant agencies. Evidence should be preserved without forwarding harmful content more widely.

A suspected personal-data breach must be reported immediately to the Headteacher and Data Protection Lead so that it can be contained, assessed and managed within the required timescales.

13 Non-Compliance

Breaches by staff, governors, volunteers or contractors may be addressed under the relevant disciplinary, conduct, capability or contractual procedure. Breaches by pupils will be managed under the Behaviour and Online Safety policies. The school will consider context, intent, impact, safeguarding and any legal duties when deciding its response.

14 Monitoring and Review

The school may monitor its official accounts, mentions of the school and publicly available content where there is a legitimate safeguarding, security or reputational reason to do so. Monitoring will be proportionate and lawful.

This policy will be reviewed annually and sooner following a serious incident, a significant change in platforms or school practice, or a material change in legislation or statutory guidance.