



Pope Francis
Catholic Multi Academy Trust

Social Media Policy

JOY MERCY SERVICE DIGNITY SOLIDARITY

Approved by:	Trust Board	
Date reviewed:	17 July 2026	
Next review due by:	16 July 2027	
Record of changes		
Date:	Name:	Changes:

Contents:

1. Purpose	3
2. Scope	3
3. Related Policies	3
4. Legal Framework	3
5. Core Principles	3
6. Roles and Responsibilities	4
7. Acceptable Use	4
8. Unacceptable Use	4
9. Safeguarding	4
10. Online Safety, Filtering and Monitoring	5
11. Data Protection and Use of Images	5
12. Professional Conduct and Boundaries	5
13. Use of Messaging Platforms	5
14. School Social Media Accounts	6
15. Personal Use of Social Media	6
16. Expectations for Parents and Carers	6
17. Safer Recruitment and Online Checks	6
18. Incident Management and Reporting	7
19. Monitoring and Compliance	7
20. Staff Wellbeing and Communication Expectations	7
21. Training	7
22. Review	8
Appendix A – Social Media Consent Form (Parents/Carers)	9
Appendix B – Inappropriate Content / Incident Report Form	10
Appendix C – Social Media Account Approval Form	11
Appendix D – Messaging Group Setup Checklist	12

1. Purpose

This policy provides a comprehensive framework to ensure the safe, professional and lawful use of social media and messaging platforms across the Trust. It supports safeguarding, protects personal data, and maintains the reputation of the Trust.

The Trust recognises that online behaviour is an integral part of safeguarding culture. All members of the school community share responsibility for maintaining safe, professional and appropriate conduct online in order to safeguard children and protect others from harm.

2. Scope

This policy applies to all staff, governors, directors, contractors, pupils and parents. It covers:

- official school or Trust social media accounts
- personal use where it impacts the Trust or school community
- messaging platforms, including WhatsApp and similar applications

3. Related Policies

This policy must be read alongside:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Data Protection Policy
- ICT Acceptable Use Policy
- Behaviour Policy
- Disciplinary Procedures

4. Legal and Regulatory Framework

This policy complies with:

- UK GDPR and Data Protection Act 2018
- Keeping Children Safe in Education (KCSIE)
- Equality Act 2010
- Safeguarding Vulnerable Groups Act 2006
- Computer Misuse Act 1990
- Freedom of Information Act 2000

5. Core Principles

All use of social media and messaging platforms must:

- be professional, respectful and appropriate
- safeguard children and vulnerable individuals

- protect confidentiality and personal data
- comply with legal and regulatory requirements
- maintain appropriate professional boundaries
- avoid bringing the Trust into disrepute

Safeguarding is everyone's responsibility and all online activity must reflect the Trust's commitment to protecting children and maintaining a safe environment.

6. Roles and Responsibilities

- Trust Board/Governing Body: ensure effective implementation and compliance
- Headteacher/Principal: oversee implementation and operational management
- Designated Safeguarding Lead (DSL): lead on safeguarding concerns and responses
- Staff: adhere to this policy and report concerns promptly
- Parents, pupils and other users: follow expected standards of behaviour

7. Acceptable Use

Social media and messaging platforms may be used for:

- communication with parents and stakeholders
- sharing appropriate information and updates
- celebrating achievements
- operational or time-sensitive communication

Messaging platforms may support communication but must not replace formal school systems.

8. Unacceptable Use

It is not permitted to:

- share confidential or personal data
- discuss individuals inappropriately
- report or manage safeguarding concerns via messaging
- post offensive, discriminatory or inappropriate content
- share images without appropriate consent or lawful basis
- engage in bullying, harassment or intimidation

9. Safeguarding

All safeguarding concerns must be reported through formal procedures in line with safeguarding policy.

Social media and messaging platforms must never be used to:

- report safeguarding concerns
- manage safeguarding incidents
- discuss sensitive safeguarding information

10. Online Safety, Filtering and Monitoring

The Trust will maintain appropriate filtering and monitoring systems to safeguard users. Leaders and DSLs will:

- understand filtering and monitoring systems
- respond to concerns promptly
- ensure emerging risks (including new technologies) are actively managed

11. Data Protection and Use of Images

Personal data, including images, must:

- be processed with a lawful basis under UK GDPR
- be used fairly, securely and appropriately
- minimise identification risks where possible

Where individuals are identifiable:

- consent or an appropriate lawful basis must be established
- individuals must be informed how their data will be used

12. Professional Conduct and Boundaries

Staff must:

- maintain clear professional boundaries at all times
- not communicate with pupils via personal social media or messaging apps unless explicitly authorised
- avoid personal online relationships with pupils or inappropriate engagement with parents
- recognise that activity on professional networking sites, including LinkedIn, may be viewed as an extension of their professional role and should conduct themselves accordingly

13. Use of Messaging Platforms

Messaging platforms (e.g. WhatsApp) must:

- have a clear purpose
- have a named administrator
- have appropriate and controlled membership
- be used professionally at all times

They must not be used to:

- share safeguarding or confidential information
- discuss individuals inappropriately
- make or record formal decisions

All formal decisions must be recorded through official school or Trust systems in line with governance and record-keeping requirements.

14. School Social Media Accounts

Official accounts must:

- be approved by senior leadership
- have secure access and password control
- be managed only by authorised staff
- be monitored and moderated appropriately
- reflect the values and reputation of the Trust

Appropriate records of account access and activity should be maintained.

15. Personal Use of Social Media

Staff personal use must:

- not impact professional responsibilities
- not damage the Trust's reputation
- not breach confidentiality
- not identify pupils, parents or school matters

Staff should use appropriate privacy settings but remain aware that online content may become public.

LinkedIn and Professional Networking Platforms

LinkedIn and other professional networking platforms are recognised as valuable tools for professional development and recruitment. Staff are encouraged to use these platforms professionally; however:

- employees must make it clear when views expressed are their own and not those of Pope Francis Catholic Multi Academy Trust
- staff must not disclose confidential or commercially sensitive information relating to the Trust or its schools
- staff must not comment publicly on matters that could prejudice Trust business, employment matters, complaints, investigations or legal proceedings
- senior leaders should take particular care as their profiles may reasonably be interpreted as representing the Trust
- use of the Trust's name, logo or branding on personal profiles must be appropriate and not imply official endorsement unless authorised

16. Expectations for Parents and Carers

Parents and carers are expected to use social media responsibly in relation to the school community.

This includes:

- not sharing images or personal information without consent
- not posting negative, harmful or defamatory content about the school, staff or pupils
- not using social media as a primary route to raise concerns

Concerns should be raised through formal school procedures so they can be addressed appropriately.

17. Safer Recruitment and Online Checks

The Trust may carry out online searches of shortlisted candidates as part of safer recruitment processes, in line with safeguarding guidance.

These checks will:

- be proportionate
- focus on publicly available information
- comply with data protection requirements

18. Incident Management and Reporting

All concerns or incidents must be reported promptly to a senior leader or DSL.

Incidents will be investigated and managed in line with safeguarding, disciplinary and data protection procedures.

Escalation will be proportionate to severity and may include:

- DSL – safeguarding concerns
- Senior Leadership Team – conduct or operational concerns
- HR – disciplinary matters
- External agencies (e.g. Local Authority, Police) where required

19. Monitoring, Audit and Compliance

The Trust reserves the right to monitor use of its systems.

To demonstrate compliance, the Trust will maintain appropriate records, including:

- approval of social media accounts
- incident reports and outcomes
- staff training and awareness records

These records provide an audit trail to support accountability and inspection readiness.

20. Staff Wellbeing and Communication Expectations

The use of messaging platforms must support and respect staff wellbeing.

- Out-of-hours communication should be limited to urgent matters
- Expectations around response times must be reasonable

21. Training

The Trust will provide regular training for staff on:

- safeguarding and online safety
 - data protection and GDPR
 - professional conduct online
- Pupils and parents will also be supported to use social media safely and responsibly.

22. Review

This policy will be reviewed regularly and updated to reflect:

- changes in legislation and guidance
- emerging risks
- best practice developments

Appendix A – Social Media Consent Form (Parents/Carers)

Pupil Name	
Year Group / Class	

I give permission for the school to use images / videos of my child for the following purposes (please tick):

School website	
School social media accounts	
Printed publications (e.g. newsletters)	
Internal displays	

I understand that:

- Images / videos may be used to promote the school
- My child's full name will not be used alongside images
- I can withdraw consent at any time in writing

Name	
Signature	
Date	

Appendix B – Inappropriate Content / Incident Report Form

Name of person reporting	
Date	

Name of individual(s) involved (if known)	
Platform (e.g. WhatsApp, Facebook)	
Description of incident:	
Immediate actions taken:	

Reported to DSL / SLT):	
Outcome / action required:	

Appendix C – Social Media Account Approval Form

Proposed account / platform:	
Purpose of account:	
Target audience:	

Named administrator(s):	
Approved by Headteacher / SLT:	
Date approved:	

Appendix D – Messaging Group Setup Checklist

Please tick	
Clear purpose defined	
Named administrator assigned	
Membership appropriate and reviewed	
No safeguarding / confidential information shared	
Group follows professional conduct expectations	
Alternative formal communication method identified	