Thames View Infants
Social Networking Policy

1. Introduction

This Policy applies to all employees, governors, volunteers, students on placement, and any adults working on behalf of the School ("staff" for brevity).

It should be read alongside the School's:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Acceptable Use / Online Safety Policy
- Disciplinary and Whistleblowing Procedures

Social media and online platforms can provide positive opportunities for communication and engagement. However, their use also presents risks, particularly in relation to safeguarding, confidentiality, and the School's reputation.

This Policy sets out clear expectations to protect pupils, staff, and the School.

2. Scope

This Policy applies to:

- Use of **social media and messaging platforms**, whether for **professional or personal purposes**
- Use **inside and outside working hours**, where activity may impact the School, its pupils, or staff
- All platforms where content can be created, shared, commented on, "liked", or responded to

This includes (but is not limited to): Facebook, WhatsApp, Instagram, TikTok, X, Bluesky, Snapchat, YouTube, blogs, forums, messaging apps, and direct messages.

3. Key Principles

Staff must ensure that their online activity:

- Safeguards children at all times
- Maintains professional boundaries
- Protects confidential and personal data
- Upholds the reputation and values of the School
- Complies with UK law, including UK GDPR and the Data Protection Act 2018

Staff should assume that **anything shared online could become public**, regardless of privacy settings.

4. Personal Use of Social Media

Staff are permitted to use personal social media accounts outside of directed hours, but must do so responsibly. Staff are personally responsible for ensuring their personal and professional social media activity is in line with the School's policies and procedures.

Staff **must not**:

- Post, share, comment on, or "like" content that could reasonably bring the School, pupils, colleagues, governors, or the wider community into disrepute
- Share, comment on, or allude to confidential, official, or sensitive information relating to the School, pupils, parents, or staff
- Discuss safeguarding matters, incidents, complaints, or internal school processes
- Post images of pupils or school activities
- Engage in abusive, discriminatory, offensive, or defamatory behaviour

Staff should:

- Keep personal accounts set to private wherever possible
- Be mindful of their role as a trusted professional within the community
- Ensure personal views cannot be mistaken as representing the School
- Report or whistle blow any concerns or wrongdoing

Where a personal account identifies the staff member as working at the School, staff are **strongly advised** to include a disclaimer stating that views are their own and do not represent those of the School.

Personal social media use during the working day must not interfere with duties and should be restricted to break times.

5. Professional Boundaries and Contact with Pupils

To safeguard children and staff:

- Staff must **not interact with pupils (past or present), or their siblings**, via personal social media or messaging apps
- Staff must not accept or initiate "friend", "follow", or messaging requests from pupils
- Any attempt by a pupil to contact a member of staff online must be reported immediately to the Headteacher or DSL
- Staff must not offer educational support, advice, or reassurance to pupils via social media or messaging platforms

- Staff must report any contact made by pupils or siblings, or any inappropriate online activity identified as being linked to a pupil or sibling (including cyber bullying), to the School's Safeguarding Team

All communication with pupils and parents must take place through **school-approved systems and channels only**. Failure to do so may result in disciplinary action being taken.

6. Contact with Parents and the School Community

- Staff are discouraged from accepting parents as contacts on personal social media accounts
- Professional communication with parents must take place through agreed school systems
- Staff should avoid online discussions about school matters, events, or individuals
- Staff must maintain professional boundaries with families they may already know personally outside of their School role
- Any concerns should be reported immediately to the School's Leadership or Safeguarding teams

7. Official School Social Media Accounts

Only social media accounts **approved by the Headteacher** may be used to represent the School.

For official accounts:

- Only authorised staff may post or manage content
- Accounts must use official school email addresses
- Content must be professional, factual, inclusive, and aligned with school values
- Posts must not include personal opinions, political views, or promotional content
- Images of pupils must comply with parental consent and the School's Online Safety Policy

8. Images, Video, and Data Protection

- Staff must not store pupil images on personal devices unless explicitly authorised
- Any authorised images must be transferred securely and deleted from personal devices promptly
- Staff must comply with UK GDPR, data protection, and information security requirements at all times.

9. Political Neutrality

Staff must ensure that personal online activity does not compromise the School's political neutrality.

Staff in politically restricted roles must not publicly support political parties or candidates. All staff must ensure that political views expressed online cannot reasonably be interpreted as representing the School.

10. Reporting Concerns

Staff must report:

- Any concerning online behaviour involving pupils and their families
- Inappropriate contact between staff and pupils
- Social media content that may pose a safeguarding or reputational risk

Concerns should be reported to the Headteacher, DSL, or line manager without delay.

11. Breaches of This Policy

Failure to comply with this Policy may result in disciplinary action, in line with the School's Disciplinary Procedures.

Serious breaches — including safeguarding failures, confidentiality breaches, or behaviour that damages the School's reputation — may constitute **gross misconduct** and could result in dismissal.

12. Review

This Policy will be reviewed regularly to ensure it remains compliant with legislation, safeguarding guidance, and best practice.