

Social Networking Policy

Version 3.0

1. Introduction

Pele Trust and its schools recognise and embrace the numerous benefits and opportunities that social media offers. While employees are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are associated risks, especially around safeguarding, bullying and personal reputation.

For the purposes of this policy, "social media" is a broad term for any kind of online platform which enables people to interact directly with each other and to share information, ideas and views. Examples include, but are not limited to, WhatsApp, Messenger, blogs, Facebook, TikTok, LinkedIn, X (formerly Twitter), Snapchat, Telegram, Threads, Google platforms, Instagram, Flickr and YouTube, and professional body sites. New and emerging platforms are automatically within the scope of this policy.

2. Scope

This policy applies to all employees, including agency workers, self-employed contractors and volunteers, and also to Directors and Academy Committee members; does not form part of any employee's contract of employment and may be amended at any time; should be read in conjunction with the Pele Trust Staff Code of Conduct; covers personal use of social media as well as use for official Pele Trust or school purposes; and includes personal communications via social media accounts that are likely to have a negative impact on professional standards or the school or Trust's reputation.

3. Purpose

The purpose of this policy is not to restrict an individual's use of social media; the Trust and its schools recognise the value of these platforms as communication and engagement tools and use them for those purposes. The purpose is to encourage good practice, to protect Pele Trust, its schools and its employees, and to promote the effective and safe use of social media as part of Trust and school activities. This policy sets clear guidelines about what is and is not appropriate use.

The policy applies regardless of whether social media is accessed using school IT facilities and equipment or equipment belonging to members of staff, and regardless of whether the use occurs during or outside the Trust or school's usual hours of operation.

4. Roles and responsibilities

Employees (including agency workers) should:

- maintain professional boundaries with pupils at all times and never communicate with current pupils via social media (with the exception of family members and, where there is a genuine need, the children of close family friends);

- not post any personal information that could jeopardise their own, their colleagues' or their family's privacy or identity, and not post any personal information about pupils, parents or other parties within the school community;
- not use their work email address when registering for, or posting on, any websites in a personal capacity;
- not use the school or Trust logo on a personal site;
- remain professional and within the boundaries of the topic being discussed when using professional body message boards, forums or sites such as LinkedIn;
- be aware of their online reputation and recognise that their online activity can be seen by others, including parents, pupils and colleagues;
- be aware that their own online presence and content can reflect on Pele Trust and its schools;
- be conscious at all times of the need to keep personal and professional lives separate, and not put themselves in a position where there is a conflict between their work and personal interests;
- ensure that any use of social media is carried out in line with this policy and other relevant policies, such as the Code of Conduct and Acceptable Use of IT;
- be aware that excessive use of social media in school may result in disciplinary action; and
- be responsible for their words and actions in an online environment: consider whether any comment, photograph or video is something you would want pupils, colleagues or other employees of the Trust to see. If in doubt, do not post it.

Directors, Academy Committee members and contractors should: conduct themselves online in a way that upholds the reputation of Pele Trust and its schools; avoid commenting publicly on school or Trust matters through personal accounts unless specifically authorised; and refrain from posting, forwarding or endorsing content that could reasonably be considered discriminatory, offensive, defamatory, misleading or otherwise damaging to the Trust, its schools or individuals.

School leaders are responsible for: disseminating this policy to all staff (for example during induction, at staff meetings and through CPD); addressing any concerns about inappropriate use of social media by colleagues; responding to concerns or questions from employees; operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them; and escalating concerns to the Headteacher where necessary (or to the CEO where concerns relate to the Headteacher).

5. Acceptable use

Employees should be aware that content uploaded to social media is not private. Even if restricted to "friends", it can be saved, forwarded, changed and reposted or distributed beyond the intended recipients. Employees using social media should therefore conduct themselves with professionalism. Employees should not upload any content that:

- is confidential to the Trust or school, its staff, its pupils or parents, or its suppliers, customers or contractors;
- refers to the Trust or school, its staff or governors, its pupils or parents, its clients, or its suppliers and contractors;
- uses the Trust or school logos;
- amounts to bullying, or to unlawful discrimination, harassment or victimisation;
- brings the Trust or school into disrepute or undermines the reputation of the Trust, school or individuals;
- contains lewd, sexually explicit, threatening or offensive language, comments, images or video clips, or similarly inappropriate material;
- is discriminatory or offensive about work colleagues;
- is defamatory or knowingly false;
- breaches copyright; or
- is in any other way unlawful.

Where the school has its own official social media accounts, posting can only be undertaken by staff authorised by the Headteacher and in accordance with this policy. Due consideration must be given to UK GDPR when posting photographs of pupils.

The Trust accepts that some employees will have family or close personal friends who are also parents of current pupils; employees are advised, rather than directed, not to accept or invite requests from parents of current pupils on their personal social media accounts. All electronic communication with parents should be through work email or official platforms in use (such as Dojo or Tapestry); where communication takes place via social media, for example on school trips, it must be through the Trust or school's accounts.

Communication via social media may occur between employees and their own family and close friends (who may also be pupils or parents), but the intent of this policy still applies, and content shared with close or personal friends will not be a reasonable defence should posts breach the acceptable use standards. Employees should be aware of professional and social boundaries and should not accept or invite friend requests from, or communicate directly via social media with, pupils or ex-pupils under the age of 18. The use of social media accounts during lesson time is not permitted unless for official or school-related purposes.

6. Safeguarding

The use of social networking sites introduces a range of potential safeguarding risks to children and young people, including online bullying; grooming, exploitation or stalking; exposure to inappropriate material or hateful language; and the encouragement of violent behaviour, self-harm or risk-taking.

To mitigate these risks: do not use any online information in an attempt to locate or meet a child; ensure that any messages, photos or information comply with existing policies; report any content or online activity which raises a safeguarding concern to the Designated Safeguarding Lead or Headteacher as soon as it is identified, as urgent steps may be needed to support and protect the young person; and, with regard to personal safeguarding, report any harassment or abuse you receive online while using your work accounts.

7. Online abuse of staff: reporting, responding and recording

Staff should never engage with cyberbullying incidents. If, in the course of your employment, you discover a website containing inaccurate, inappropriate or inflammatory material relating to you, or images of you taken or used without your permission, you should immediately report this to the Headteacher. Staff should keep records of abuse (texts, emails, voicemail, website or social media content); where appropriate, screenshots should be taken and the time, date and address of the site recorded.

The Trust will support staff in addressing online abuse or harmful content. This may include: assisting staff to use the relevant platform's complaints or takedown procedures; escalating concerns to the platform provider on behalf of staff; where appropriate, reporting content to the police or other relevant external agencies; and offering pastoral and professional support to staff affected by online abuse.

Online harassment of staff by third parties falls within the Trust's duty not to permit the harassment of its staff and dealing with such conduct may result in third parties facing restrictions on access to school sites and communication channels, reports to platforms, or referral to the police.

8. Action by employer: inappropriate use of social media

Following a report of inappropriate use of social media, a senior leader will conduct a prompt initial investigation. Any member of staff suspected of committing a breach of this policy (or about whom complaints of unacceptable use are received) may be investigated in accordance with the Pele Trust Disciplinary Policy and/or Anti-harassment and Bullying Policy. If the outcome of an investigation leads to disciplinary action, serious breaches could result in dismissal. Where conduct is considered unlawful, the Trust will report the matter to the police and other relevant

external agencies. In the case of agency workers or contractors, the incident will be reported to the agency and the assignment or works order may be terminated.

9. Monitoring

All Pele Trust and school ICT systems may be monitored in accordance with the ICT Security Policy, so personal privacy cannot be assumed when using school devices and networks. Schools can monitor the usage of their own internet and email services when justifiable concerns have been raised. Any targeted monitoring of an individual will be authorised by the Headteacher or the Chief Operating Officer, recorded, and limited to what is necessary and proportionate to the concern, in line with ICO guidance.

Pele Trust respects the privacy of its employees. However, postings made on a personal account may attain a wide readership and will therefore be considered public rather than private. Publicly accessible postings may be investigated if there is a suspected breach of this or related policies.

10. Legislation

In applying this policy, the school and Trust will adhere to their rights, responsibilities and duties in accordance with the following:

- the Online Safety Act 2023;
- the Investigatory Powers Act 2016;
- UK GDPR and the Data Protection Act 2018;
- the Human Rights Act 1998;
- the Equality Act 2010;
- the Defamation Act 2013; and
- Keeping Children Safe in Education (current edition).

And with Pele Trust's own policies, including the Staff Code of Conduct, the Disciplinary Policy, the Anti-harassment and Bullying Policy, school Acceptable Use and IT Security policies, and Safer Recruitment guidance.

The internet is a fast-moving technology and it is impossible to cover all circumstances or potential issues; the principles set out in this policy must be followed irrespective of the medium. When using social media, staff should be aware of the potential impact on themselves and the employer, whether for work-related or personal use, during working hours or otherwise, and whichever equipment is used. Staff should use discretion and common sense when engaging in online communication.

Helpful general guidance:

[Social Media: how to use it safely](#) (National Cyber Security Centre);

Document control

Version	Version 3.0
Status	Issued September 2026
Next review	September 2027
Approved by	Board of Directors

Version	Date	Notes
3.0	September 2026	Legislation list updated: Online Safety Act 2023 added; Investigatory Powers Act 2016 replaces RIPA 2000; KCSIE reference made edition-proof. Online abuse of staff by third parties connected to the Trust's duty not to permit third-party harassment (Employment Rights Act 2025) Targeted monitoring now requires authorisation, recording and proportionality in line with ICO guidance.
2.2	September 2025	Policy scope extended to agency workers and contractors; inclusion of Trust support for victims of cyberbullying; updated legislation.
2.1	November 2024	Examples of social media platforms updated to include WhatsApp and Messenger.
2.0	September 2024	Format updates.
1.0	March 2023	Adopted by Directors.