



Social Media Policy

Approved by:
B.Suddhi

Date: February 2026

Last reviewed on: February 2026

Next review due February 2027
by:

Signed by:

Headteacher

Date: February 2026

Chair of governors

Date: February 2026

Contents:

- Statement of intent
- Legal framework
- Roles and responsibilities
- Definitions
- Data protection principles
- School Social media accounts
- Social media use – staff
- Social media use – pupils
- Social media use – parents
- Online safety
- Blocked content
- Cyber bullying
- Training
- Monitoring and review

Statement of intent

Pear Tree Infant and Nursery school understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

We are committed to:

- Encouraging the responsible use of social media by all staff, parents and pupils in support of the school's mission, values and objectives.
- Protecting our pupils from the dangers of social media.
- Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- Protecting our staff from cyber bullying and potentially career damaging behaviour.
- Arranging e-safety meetings for parents.

1. Legal framework

1.1. This policy has due regard to legislation and guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- DfE (2023) 'Data protection in schools' (2025 update)
- The Data Protection Act 2018
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- The Freedom of Information Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- DfE (2025) 'Keeping Children Safe In Education 2025'

1.2. This policy will be implemented in accordance with the following school policies and documents:

- Data and E-Security Breach Prevention and Management Plan
- Acceptable use of Devices Policy
- Data Protection Policy
- Complaints Procedures Policy
- Staff Code of Conduct
- Confidentiality Policy
- Child Protection and Safeguarding Policy
- Disciplinary Policy and Procedures
- Behavioural Policy

2. Roles and responsibilities

2.1. The headteacher is responsible for:

- The overall implementation of this policy and ensuring that all staff, parents and pupils are aware of their responsibilities in relation to social media use.
- Promoting safer working practices and standards with regards to the use of social media.
- Establishing clear expectations of behaviour for social media use.
- Ensuring that this policy, as written, does not discriminate on any grounds, including, but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- In conjunction with the governing board, handling complaints regarding this policy and its provisions in line with the school's Complaints Procedures Policy.

- Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.
- Taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use.
- Working alongside the data protection officer (DPO) to ensure appropriate security measures are implemented and compliance with the GDPR.

2.2. Staff members are responsible for:

- Adhering to the principles outlined in this policy.
- Reporting any social media misuse by staff, pupils or parents to the headteacher immediately.
- Attending any training on social media use offered by the school.

2.3. Parents are responsible for:

- Adhering to the principles outlined in this policy.
- Taking appropriate responsibility for their use of social media and the influence on their children at home.
- Promoting safe social media behaviour for both themselves and their children.
- Attending e-safety meetings held by the school wherever possible.

2.4. Governing body are responsible for:

- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.

2.5. ICT Technicians are responsible for:

- Providing technical support in the development and implementation of the school's social media accounts.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

2.6. The DLS will be responsible for:

- The school's approach to online safety
- Dealing with concerns about social media use that are safeguarding concerns

• Definitions

- For the purpose of this policy, the school defines “**social media**” as any online platform that offers real-time interaction between the user and other individuals or groups including, but not limited to, the following:
 - Blogs
 - Online discussion forums, such as netmums.com
 - Collaborative spaces, such as Facebook, Instagram
 - Media-sharing devices, such as YouTube
 - ‘Micro-blogging’ applications, such as Twitter
- For the purpose of this policy, “**cyber bullying**” is defined as any social media or communication technology intentionally used to bully an individual or group, including the posting or sharing of messages, images or videos.
- For the purpose of this policy, “**members of the school community**” are defined as any teacher, member of support staff, pupil, parent of a pupil, governor or ex-pupil.

• Data protection principles

- The school will obtain consent from pupils and parents at the beginning of each academic year using the Images and Videos Parental Consent Form, which will confirm whether or not consent is given for posting images and videos of a pupil on social media platforms. The consent will be valid for the entire academic year.
- A record of consent is maintained throughout the academic year, which details the pupils for whom consent has been provided. The DPO is responsible for ensuring this consent record remains up-to-date.
- For the purpose of section 4.1, where a pupil is assessed by the school to have the competence to understand what they are consenting to, the school will obtain consent directly from that pupil; otherwise, consent is obtained from whoever holds parental responsibility for the child.
- Parents and pupils are able to withdraw or amend their consent at any time. To do so, parents and pupils must inform the school in writing.
- Consent can be provided for certain principles only, for example only images of a pupil are permitted to be posted, and not videos. This will be made explicitly clear on the consent form provided.
- Where parents or pupils withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents’ and pupils’ requirements following this.

- In line with section 4.5, wherever it is reasonably practicable to do so, the school will take measures to remove any posts before consent was withdrawn or amended, such as removing an image from a social media site.
- The school will only post images and videos of pupils for whom consent has been received.
- Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved by the headteacher for use.
- When posting images and videos of pupils, the school will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a pupil being identified.
- The school will not post pupils' personal details on social media platforms.
- Pupils' full names will never be used alongside any videos or images in which they are present.
- Only appropriate images and videos of pupils will be posted in which they are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.
- When posting on social media, the school will use group or class images or videos with general labels, e.g. 'sports day'.
- Consent provided for the use of images and videos only applies to school accounts – staff, pupils and parents are not permitted to post any imagery or videos on personal accounts.

• **School Social Media Accounts**

Social media accounts for the school will only be created by the School Business Manager and other designated staff members, following approval from the headteacher. A school-based social media account will be entirely separate from any personal social media accounts held by staff members and will be linked to an official school email account.

When setting up a school social media account, consideration will be given to the following:

- The purpose of the account
- Whether the overall investment will achieve the aim of the account
- The level of interactive engagement with the site
- Whether pupils, staff, parents or members of the public will be able to contribute content to the account
- How much time and effort staff members are willing to commit to the account
- How the success of the account will be evaluated

The headteacher will be responsible for authorising members of staff and any other individual to have admin access to school social media accounts. Only people authorised by the headteacher will be allowed to post on the school's accounts.

Passwords for the school's social media accounts are stored securely on the school's ICT network. The passwords are only shared with people authorised by the headteacher.

All posts made to school social media accounts will not breach copyright, data protection or freedom of information legislation.

Staff will ensure any posts are positive in nature and relevant to pupils, the work of staff, the school or any achievements.

Staff will not post any content online which is damaging to the school or any of its staff or pupils.

The school's social media accounts will comply with the platform's rules. The School Business Manager will ensure anyone with authorisation to post on the school's social media accounts are provided with training on the platform and the rules around what can be posted.

School social media accounts will be moderated by the School Business Manager or another designated member of staff.

• **Social media use – staff**

Personal accounts

Staff will not be prohibited from having personal social media accounts; however, it is important that staff protect their professional reputation by ensuring they use personal social media accounts in an appropriate manner

- Staff members will not access social media platforms during lesson times.
- Staff members will not use any school-owned mobile devices to access personal accounts, unless it is beneficial to the material being taught – prior permission will be sought from the headteacher.
- Staff members are permitted to use social media during break times.
- Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the headteacher.
- Staff will avoid using social media in front of pupils.
- Staff will not "friend" or otherwise contact pupils or parents through their personal social media accounts.
- If pupils or parents attempt to "friend" a staff member they will report this to the headteacher.
- Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with pupils or parents will be done through authorised school contact channels.

- Staff members will ensure the necessary privacy controls are applied to personal accounts.
- Staff members' personal information will not be discussed on social media.
- No staff member will post any content online that is damaging to the school or any of its staff or pupils.
- Social media will not be used as a platform to attack, insult, abuse or defame pupils, their family members, colleagues or other professionals.
- Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not that of the school.
- Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.
- Staff will not take any posts, images or videos from social media that belong to the school for their own personal use.
- Staff members will not post anonymously or under an alias to evade the guidance given in this policy.
- Staff will not post comments about the school, pupils, parents, staff or other members of the school community.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.
- Members of staff will regularly check their online presence for negative content via search engines.
- Attempts to bully, coerce or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.
- Members of staff will not leave a computer or other device logged in when away from their desk or save passwords.
- Staff members will use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

• **Pupil social media use**

- Pupils will not access social media during lesson time, unless it is part of a curriculum activity. Pupils will not be permitted to use the school's WiFi network to access any social

media platforms unless prior permission has been sought from the headteacher, and an ICT technician has ensured appropriate network security measures are applied.

- Pupils will not attempt to 'friend', 'follow' or otherwise contact members of staff through their personal social media accounts. Where a pupil attempts to 'friend' or 'follow' a staff member on their personal account, it will be reported to the headteacher.
- Pupils will not post any content online which is damaging to the school or any of its staff or pupils. Pupils will not post anonymously or under an alias to evade the guidance given in this policy.
- Pupils are instructed not to sign up to any social media platforms that have an age restriction above the pupil's age.
- If inappropriate content is accessed online on school premises, this will be reported to a member of staff.
- Breaches of this policy will be taken seriously, and managed in line with the Behaviour Policy.

• **Parent social media use**

Parents are able to comment on or respond to information shared via social media sites; however, parents should do so in a way which does not damage the reputation of the school.

Parents will be asked not to share any photos or personal details of pupils when commenting on school social media sites, nor post comments concerning other pupils or staff members.

Any parents that are seen to be breaching the guidance in this policy will be required to attend a meeting with the headteacher, and may have their ability to interact with the social media websites removed.

Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution.

• **Online safety - Safeguarding**

Any disclosures made by pupils to staff about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour will be reported to the headteacher, who will decide on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it will be reported to the chair of governors.

Concerns regarding a pupil's online behaviour will be reported to the DSL, who will investigate any concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher will contact the police. The school will avoid unnecessarily criminalising pupils, e.g. calling the police, where

criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy

• **Blocked content**

- In accordance with the school's Data and E-Security Breach Prevention and Management Plan, the e-safety officer installs firewalls on the school's network to prevent access to certain websites. The following social media websites are not accessible on the school's network:
 - Twitter (X)
 - Facebook
 - Instagram
- Attempts made to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.
- Inappropriate content accessed on the school's computers will be reported to the headteacher so that the site can be blocked.
- The headteacher retains the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

• **Cyber bullying**

- Allegations of cyber bullying from staff members will be handled in accordance with policy.
- Staff members will not respond or retaliate to cyber bullying incidents. Incidents will be reported as inappropriate, and support will be sought from the headteacher.
- Evidence from the incident will be saved, including screen prints of messages or web pages, and the time and date of the incident.
- Where the perpetrator is a colleague, most incidents can be handled through the school's own disciplinary procedures.
- Where the perpetrator is an adult, in nearly all cases, a member of the SLT will invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.
- If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms if the offensive content breaches their terms and conditions.

- If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school will consider whether the police should be contacted.
- As part of the school's ongoing commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and PSHE.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. Allegations of cyberbullying from staff members will be handled in accordance with the Allegations of Abusive Parents Policy.

- **Training**

- 2.7. At Pear Tree Infant and Nursery school we recognise that early intervention can protect pupils who may be at risk of cyber bullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk pupils.
- 2.8. Teachers and support staff will receive training on the Social Media Policy as part of their new starter induction.
- 2.9. Teachers and support staff will receive ongoing training as part of their development.
- 2.10. Pupils will be educated about e-safety and appropriate social media use on a termly basis through a variety of mediums, including: assemblies, PSHE lessons and cross-curricular links.
- 2.11. Training for all pupils, staff and parents will be refreshed in light of any significant incidents or changes.

- **Monitoring and review**

- This policy will be reviewed on an annual basis by the headteacher, in conjunction with the School Business Manager and DPO.
- The next scheduled review date for this policy is February 2027.
- Any changes made to this policy will be communicated to all staff, pupils and parents.