Rosehill School

Social Media Policy

Policy lead:	**Headteacher, Computing Lead**
Date written:	**April 2026**
Review date:	**April 2027**
Approval status	**Approved at full governing body meeting 6.5.2026**

Contents:

Statement of intent

Rosehill 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 cyberbullying and potentially career damaging behaviour.
- Arranging online safety meetings for parents.

1. Legal framework

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

- DfE (2018) 'Data protection: a toolkit for schools'
- The UK General Data Protection Regulation (UK GDPR)
- 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
- Keeping Children Safe in Education 202024
- DfE (2024) Filtering and Monitoring Standards for Schools and Colleges guidance
- KCSIE (latest version)

1.2 This policy operates in conjunction with the following school policies:

- Home-School Agreement
- Acceptable Use Policies – Pupils
- Staff ICT & Devices, Including Acceptable Use Agreement
- Pupil Devices, Including Acceptable Use Agreement
- ESafety Policy
- GDPR Data Protection Policy
- Positive Behaviour Support and Physical Intervention Policy
- Complaints Procedures Policy
- Anti-bullying Policy
- Disciplinary Procedures – Staff Facing Allegations of Abuse Policy
- Photography Policy
- Code of Conduct Policy
- Confidentiality Agreement (Included in Visitors Policy)
- Data and Cyber-Security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- Disciplinary Procedures
- Filtering and monitoring policy
- Safe use of AI 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 against any of the protected characteristics, as outlined in the Equality Act 2010.
- 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 online safety officer and data protection officer (DPO) to ensure appropriate security measures are implemented and compliance with UK GDPR.

2.2 The governing board is 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.

2.3 Staff members are responsible for:

- Adhering to the principles outlined in this policy and the Technology Acceptable Use Agreement – Staff.
- Ensuring pupils adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom.
- 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.

2.4 Parents are responsible for:

- Adhering to the principles outlined in this policy and the Home School Agreement.
- 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 online safety meetings held by the school wherever possible.
- Not engaging in activities involving social media which might bring the school into disrepute.
- Not representing their personal views as those of the school on any social medium.
- Acting in the best interests of pupils when creating, participating in or contributing to social media sites.

2.5 Pupils are responsible for:

- Adhering to the principles outlined in this policy and the Pupil Code of Conduct.
- Ensuring they understand how to use social media appropriately and stay safe online.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Demonstrating the same high standards of behaviour as expected within the school.

2.6 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.

3. Definitions

3.1 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
- Collaborative spaces, such as Facebook
- Media-sharing devices, such as YouTube
- 'Micro-blogging' applications, such as X (Twitter)

3.2 For the purpose of this policy, **"cyberbullying"** 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.

3.3 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.

4. Data protection principles

4.1 Rosehill 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. 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.

4.2 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 pupil.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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 from provided.

4.8 The school will only post images and videos of pupils for whom consent has been received.

4.9 Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved by the online safety officer for use.

4.10 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.

4.11 When posting on social media, the school will use group or class images or videos with general labels, e.g. 'sports day'.

4.12 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.

4.13 The school will not post pupils' personal details on social media platforms and pupils' full names will never be used alongside any videos or images in which they are present.

4.14 Before posting on social media, staff will:

- Refer to the consent record log to ensure consent has been received for that pupil and for the exact processing activities required.
- Ensure that there is no additional identifying information relating to a pupil.

4.15 Any breaches of the data protection principles will be handled in accordance with the school's Data and Cyber-security Breach Prevention and Management Plan.

5. Staff social media use

School accounts

5.1 The school's social media sites will only be created and monitored by the ICT technicians and other designated staff members. There will be a strong pedagogical or

business reason for the creation of social media accounts on behalf of the school; official school profiles and accounts will not be created for trivial reasons.

5.2 A school 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.

5.3 Consideration will be given to the following aspects:

- The purpose for using social media
- Whether the overall investment will achieve the pedagogical aim
- 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 proposed site
- A clear plan which outlines aspects such as how long the site will last
- How the success of the site will be evaluated

5.4 School social media passwords are kept in the headteacher's office – these are not shared with any unauthorised persons, including pupils, unless otherwise permitted by the headteacher.

5.5 Staff will adhere to the data protection principles outlined in section 4 of this policy at all times.

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

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

5.8 All content expressed on school social media accounts will not breach copyright, data protection or freedom of information legislation.

5.9 Staff will ensure the headteacher has checked the content before anything is posted on social media.

5.10 If staff wish for reminders to be posted for parents, e.g. returning slips for a school trip, staff will seek permission from the headteacher before anything is posted.

5.11 If inappropriate content is accessed online, a report form will be completed and passed on to Headteacher. The Headteacher retains the right to monitor staff members' internet usage in line with the Data and Cyber-security Breach Prevention and Management Plan.

Personal accounts

5.12 Staff members will not access social media platforms during lesson times, but they are permitted to use social media during break times.

5.13 Staff will avoid using social media in front of pupils.

5.14 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.

5.15 Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the headteacher, and once the online safety officer has ensured the necessary network security controls are applied.

5.16 Staff will not 'friend', 'follow' or otherwise contact pupils or parents through their personal social media accounts. If pupils or parents attempt to 'friend' or 'follow' a staff member, they will report this to the headteacher.

5.17 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.

5.18 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.

5.19 Staff members will ensure the necessary privacy controls are applied to personal accounts and will avoid identifying themselves as an employee of the school on their personal social media accounts.

5.20 Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not those of the school.

5.21 No staff member will post any content online that is damaging to the school or any of its staff or pupils.

5.22 Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.

5.23 Staff will not take any posts, images or videos from social media that belong to the school for their own personal use.

5.24 Staff members will not post anonymously or under an alias to evade the guidance given in this policy.

5.25 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.

5.26 Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.

5.27 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.

5.28 Social media will not be used as a platform to attack, insult, abuse or defame pupils, their family members, colleagues or other professionals.

5.29 Staff members' personal information will not be discussed on social media.

Safer recruitment – online checks

5.30. As part of our shortlisting process we may carry out an online search as part of our due diligence for shortlisted candidates.

5.31. This would take place to assist us in identifying any incidents or issues that have happened.

5.32. This would only be information which is publicly available.

5.33. Any issues or incidents may be explored further at interview.

6. Parent social media use

6.1 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.

6.2 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, in accordance with the Home School Agreement.

6.3 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.

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

7. Pupil social media use

7.1 Pupils will not access social media during lesson time, unless it is part of a curriculum activity.

7.2 Pupils are not permitted to use the school's WiFi network to access any social media platforms unless prior permission has been sought from the headteacher, and the online safety officer has ensured appropriate network security measures are applied.

7.3 Pupils will not attempt to 'friend', 'follow' or otherwise contact members of staff through their personal social media accounts.

7.4 Pupils are only permitted to be affiliates of school social media accounts.

7.5 Where a pupil or parent attempts to "friend" or 'follow' a staff member on their personal account, it will be reported to the headteacher.

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

7.7 Pupils will not post anonymously or under an alias to evade the guidance given in this policy.

7.8 Pupils are instructed not to sign up to any social media sites that have an age restriction above the pupil's age.

7.9 If inappropriate content is accessed online on school premises, it will be reported to a teacher.

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

8. Online safety

8.1 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.

8.2 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.

8.3 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.

8.4 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.
8.5 The use of AI will be in accordance to the safer use of AI policy.

9. Blocked content

9.1 In accordance with the school's Data and Cyber-security Breach Prevention and Management Plan, the online safety officer will install 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:

- X (Twitter)
- Facebook
- Instagram

9.2 The Headteacher retains the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

9.3 Attempts made to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.

9.4 Inappropriate content accessed on the school's computers will be reported to the Computing lead so that the site can be blocked.

9.5 Requests may be made to access erroneously blocked content by submitting a blocked content access form to the Computing lead, which will be approved by the headteacher.

10. Cyberbullying

10.1 Cyberbullying incidents are taken seriously at Rosehill School. Any reports of cyberbullying on social media platforms by pupils will be handled in accordance with the Anti-bullying Policy.

10.2 Cyberbullying against pupils or staff is not tolerated under any circumstances.

10.3 Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

10.4. 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.

10.5 Evidence from the incident will be saved, including screen prints of messages or web pages, and the time and date of the incident.

10.6 Where the perpetrator is a current pupil or colleague, most incidents can be handled through the school's own disciplinary procedures.

10.7 Where the perpetrator is an adult, 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.

10.8 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.

10.9 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.

10.10 Allegations of cyberbullying from staff members will be handled in accordance with the Allegations of Abuse Against Staff Policy.

10.11 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.

9. Training

9.1 The school recognises that early intervention can protect pupils who may be at risk of cyberbullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk pupils.

9.2 Teachers and support staff will receive training on social media as part of their new starter induction.

9.3 Teachers and support staff will receive termly and ongoing training as part of their development.

9.4 Pupils will be educated about online safety and appropriate social media use on a termly basis through a variety of mediums, including assemblies, PSHE lessons and cross-curricular links.

9.5 Pupils will be provided with material to reinforce their knowledge.

9.6 Parents will be invited to online safety and social media training on an annual basis and provided with relevant resources, such as our Social Media Code of Conduct for Parents.

9.7 Training for all pupils, staff and parents will be refreshed in light of any significant incidents or changes.

10. Monitoring and review

10.1 This policy will be reviewed on an annual basis by the Headteacher, in conjunction with the Computing lead and DPO.

10.2 The next scheduled review date for this policy is April 2027

10.3 Any changes made to this policy will be communicated to all staff, pupils and parents.

Blocked content access request form

Requester	
Staff name:	
Date:	
Full URL:	
Site content:	
Reasons for access:	
Identified risks and control measures:	
Authoriser	
Approved?	✓ / X
Reasons:	
Staff name:	
Date:	
Signature:	

Inappropriate content report form

Staff name (submitting report):	
Name of individual accessing inappropriate content (if known):	
Date:	
Full URL(s):	
Nature of inappropriate content:	
To be completed by online safety officer	
Action taken:	
Staff name:	
Date:	
Signature:	

Social media site creation approval form

Use of social media on behalf of the school must be approved by the headteacher prior to setting up sites. Please complete this form and return it to the headteacher.

Team details		
Department:		
Moderator of site:		
Purpose of using social media		
Please describe why you want to set up this site and the content of the site		
What are your aims and what do you hope to achieve by setting up this site?		
What is the proposed content of the site?		
Proposed audience of the site		
☐ Pupils of the school Ages: age range	☐ School staff	☐ Pupils' family members
☐ External organisations	☐ Pupils from other schools Schools involved: name of school	☐ Members of the public
☐ Other (please give details)		
Proposed contributors to the site		
☐ Pupils of the school Ages: age range	☐ School staff	☐ Pupils' family members
☐ External organisations	☐ Pupils from other schools Schools involved: name of school	☐ Members of the public
☐ Other (please give details)		
Administration of the site		
Names of administrators (the site must have at least two approved administrators):		
Who will vet external contributors? (Please state name and job role)		

Who will host the site?		
Proposed date of going live:		
How do you propose to advertise for contributors?		
If contributors include pupils, how do you propose to inform and obtain the consent of parents or responsible adults?		
What security measures will you take to prevent unwanted or unsuitable individuals from contributing or becoming 'friends' and 'followers' etc. of the site?		
Approval		
Approval from relevant people must be obtained before the site can be created. The relevant managers must read this form and complete the information below before final approval can be given by the headteacher.		
Communications officer I approve the aims and content of the proposed site and the use of the school brand and logo.	Name:	
	Signature:	
	Date:	
Headteacher I approve the aims and content of the proposed site and the use of the school brand and logo.	Name:	
	Signature:	
	Date:	