Tormead School

RYDES HILL PREPARATORY SCHOOL & NURSERY

Tormead Family

Social Media Policy

This policy also applies to EYFS

Tormead Limited includes two schools with one Governing Body:

- Tormead School (Preparatory and Senior School), Cranley Rd, Guildford GU1 2JD ("Tormead") and
- Rydes Hill Preparatory School and Nursery, Aldershot Rd, Guildford GU2 8BP ("Rydes Hill")

This policy refers to both schools.

Introduction

Tormead 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. Roles and responsibilities

The Governors will be responsible for:

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

The Head will be 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.
- In conjunction with the Governors, handling complaints regarding this policy and its provisions in line with the school's Complaints Procedure.
- 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 DPO and ICT technicians to ensure appropriate security measures are implemented and compliance with UK GDPR and other data protection legislation.

The DSL will be responsible for:

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

Staff members will be responsible for:

- Adhering to the principles outlined in this policy and the Acceptable Use Agreement for 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 Head immediately.
- Attending any training on social media use offered by the school.

Parents will be 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.
- Reporting any social media misuse to the Head.
- Promoting safe social media behaviour for both themselves and their children.
- Attending meetings held by the school regarding E-Safety.

Pupils will be 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 on social media.
- Reporting incidents and concerns relating to social media in line with the procedures within this policy.
- Demonstrating the same high standards of behaviour as expected within the school.

The Deputy Head – External Relations will be responsible for:

- Monitoring and reviewing all school-run social media accounts.
- Vetting and approving individuals who wish to be 'friends' or 'followers' on the school's social media platforms.
- Consulting with staff on the purpose of the social media account and the content published.
- Maintaining a log of inappropriate comments or abuse relating to the school.
- Handling inappropriate comments or abuse posted on the school's social media accounts, or regarding the school.
- Creating a terms of use agreement, which all content published must be in accordance with.
- Ensuring that enough resources are provided to keep the content of the social media accounts up-to-date and relevant.

ICT technicians will be 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 Head.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

2. School social media accounts

Social media accounts for the school will only be created by the Deputy Head – External Relations and other designated staff members. 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 Deputy Head – External Relations 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 Head will be allowed to post on the school's accounts.

Passwords for the school's social media accounts are stored securely on BitWarden which can be accessed by the Marketing Team and ICT. The passwords are only shared with people authorised by the Deputy Head – External Relations.

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

The school's social media accounts will comply with the platform's rules. The Deputy Head – External Relations 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 Deputy Head – External Relations or another designated member of staff.

Staff conduct

Only staff with authorisation from the Deputy Head – External Relations will post on school accounts. Guidance to staff is outlined in the External Relations Instructional Staff Manual which can be found on SharePoint under All Staff/Handbooks.

Staff will have content approved by the Deputy Head – External Relations before it is posted. Staff will only post content that meets the school's social media objectives, including the following:

- Reminders about upcoming parent events e.g. open days
- Good news regarding the school's performance, attainment or reputation
- Good news regarding the achievements of staff and pupils
- Information that parents should be aware of, e.g. school closure

Staff will ensure that their posts meet the following criteria:

- The post does not risk bringing the school into disrepute
- The post only expresses neutral opinions and does not include any personal views
- The post uses appropriate and school-friendly language
- The post is sensitive towards those who will read it, and uses particularly neutral and sensitive language when discussing something that may be controversial to some
- The post does not contain any wording or content that could be construed as offensive
- The post does not take a side in any political debate or express political opinions
- The post does not contain any illegal or unlawful content

3. Staff use of personal social media

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 will be required to adhere to the following guidelines when using personal social media accounts:

- Staff members will not use any school-owned mobile devices to access personal accounts.

- Staff will not 'friend', 'follow' or otherwise contact pupils through their personal social media accounts. If pupils attempt to 'friend' or 'follow' a staff member, they will report this to the Head.
- Staff will be strongly advised to not 'friend' or 'follow' parents on their personal accounts.
- 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.
- Staff will ensure it is clear that views posted on personal accounts are personal and are not those of the school.
- Staff will not post any content online that is damaging to the school, its staff or pupils.
- 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 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.

We recognise that you may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communication systems (including via smartphones and tablets). We authorise such occasional use provided use is minimal and takes place substantially out of normal working hours (i.e. during your lunch break or before or after work) and so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and is in accordance with this Policy.

Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the School's business are also prohibited. You must ensure that your use of social media does not create any breaches of internet security and therefore must be careful to avoid any applications that might interrupt our IT systems. Excessive use of social media that interrupts productivity will be subject to a disciplinary procedure, consistent with this policy.

We prohibit you from using your work email address for any personal use of social media.

Permission to use our systems to access social media platforms for personal use may be withdrawn at any time at our discretion.

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.

4. Parent use of social media

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 Head, 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, and will be viewed as a breach of the Parent Code of Conduct.

5. Pupil use of social media

Pupils will not access social media during lesson time, unless it is part of monitored 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 Head, 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 Head.

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.

6. Data protection principles

The school will obtain consent from pupils and parents at the beginning of each academic year, 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.

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.

A record of consent is maintained throughout the academic year, which details the pupils for whom consent has been provided. The Network Manager will be responsible for ensuring this consent record remains up-to-date.

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 to the Network Manager PhotoConsent@tormeadschool.org.uk. Changes to consent may take up to 48 hours to be processed. 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. Please see the Taking, Storing and Using Images of Children Policy for more details. If a member of staff wishes to withdraw consent they should contact the Marketing Team who can either remove the image.

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. Only appropriate images and videos of pupils will be posted in which they are suitably dressed, e.g. 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'.

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 and pupils' full names will never be used alongside any videos or images in which they are present.

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.

Any breaches of the data protection principles will be handled in accordance with the school's Cyber-security Policy.

7. 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 Safeguarding Policy.

Concerns regarding a staff member's online behaviour will be reported to the Head, who will decide on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Managing Allegations, and Disciplinary Policy and Procedures. If the concern is about the Head, 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, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Head 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 Safeguarding Policy.

As part of the usual communication with parents, the school will reinforce the importance of pupils being safe online and inform parents what systems the school uses to filter and monitor online use. The school will also make it clear to parents what their children are being asked to do online for school. including what platforms they will be asked to access and who from the school, if anyone, they will be interacting with online.

8. Blocked content

In accordance with the school's Cyber-security Policy, 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 (this list is not exhaustive):

- Facebook
- Instagram
- Tik Tok
- X

ICT technicians retain the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

Attempts made to circumvent the network's firewalls may 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 an ICT technician so that the site can be blocked. Requests may be made to access erroneously blocked content by submitting a blocked content access form to an ICT technician, which will be approved by the Head.

9. Cyberbullying

Any reports of cyberbullying on social media platforms by pupils will be handled in accordance with the Anti-bullying Policy.

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 Managing Allegations Policy.

10. Training

The school recognises that early intervention can protect pupils who may be at risk of cyberbullying or negative social media behaviour. As such, staff will receive training in identifying potentially at-risk pupils. Staff will receive social media training as part of new joiner inductions and staff have access to a social media guide.

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

Parents will be invited to online safety and social media training on an annual basis and provided with relevant resources. Training for all pupils, staff and parents will be refreshed in light of any significant incidents or changes.

11. Legal framework

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

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

This policy operates in conjunction with the following school policies:

- IT Acceptable Use Agreement for Staff and Pupils
- Data Protection Policy

- Pupil Code of Conduct
- Complaints Procedure
- Anti-bullying Policy
- Cyber Security Policy
- Taking, Storing and Using Images of Children Policy
- Staff Code of Conduct
- Safeguarding Policy
- Behaviour Policy