The Robert Carre Trust

Social Media Policy

Contents:

Statement of intent

The Robert Carre Trust understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our students against potential dangers when accessing the internet at school, and to educate our students 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 students in support of the Trust's mission, values and objectives.
- Protecting our students 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.

Legal framework

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
- DfE (2023) 'Keeping children safe in education 2023'

This policy operates in conjunction with the following school policies:

- Social Media Code of Conduct for Parents
- Whole-School Social Media Accounts Policy
- Technology Acceptable Use Agreement for Staff
- Online Safety Policy
- Data Protection Policy
- Student Code of Conduct
- Complaints Procedures Policy
- Anti-bullying Policy
- Allegations of Abuse Against Staff Policy
- Photography and Images Policy
- Social Media Policy
- Acceptable Use Agreement
- Staff Code of Conduct
- Confidentiality Policy

- Data and Cyber-Security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- Disciplinary Policy and Procedure
- Behaviour Policy

Roles and responsibilities

The Executive Headteacher/ Headteacher is responsible for:

- The overall implementation of this policy and ensuring that all staff, parents and students 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 Trustees and Local Governance Tier, 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.

The Trustees and Local Governance Tier 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.

Staff members are responsible for:

- Adhering to the principles outlined in this policy and the ICT Acceptable Use Policy for Staff.
- Ensuring students 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, students or parents to the Executive Headteacher/ Headteacher immediately.
- Attending any training on social media use offered by the school.

Parents are responsible for:

- Adhering to the principles outlined in this policy and the Social Media Code of Conduct for Parents.

- 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 students when creating, participating in or contributing to social media sites.

Students are responsible for:

- Adhering to the principles outlined in this policy and the Student 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.

As communication leads, the Executive Headteacher and Headteacher are 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 Support is 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 Executive Headteacher/ Headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

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

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.

For the purpose of this policy, **"members of the school community"** are defined as any teacher, member of support staff, student, parent of a student, Trustee or Governor or ex-student.

MCAS (My Child at School) is part of Bromcom (the Trust's management information system) which allows home-school exchange of information.

Data protection principles

The school will obtain consent from students and parents on initial enrolment using MCAS which will confirm whether or not consent is given for posting images and videos of a student on social media platforms. The consent will be valid for the duration of the student's time at the school or until updated by the parent. 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.

A record of consent is maintained on MCAS detailing the students for whom consent has been provided.

Parents and students are able to withdraw or amend their consent at any time. To do so, parents and student inform the school in writing. Where parents or students 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 students' requirements following this. 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.

Consent can be provided for certain principles only, for example only images of a student are permitted to be posted, and not videos. This will be made explicitly clear on the consent from provided. The school will only post images and videos of students 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 online safety officer for use. Only appropriate images and videos of students will be posted in which they are suitably dressed, i.e., it would not be suitable to display an image of a student 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 students, the school will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a students 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 Bromcom to ensure consent has been received for that student and for the exact processing activities required.
- Ensure that there is no additional identifying information relating to a student.

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.

Staff social media use

School accounts

The school's social media sites will only be created and monitored by ICT Support. 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.

If members of staff wish to create a new social media account, they should apply to ICT Support.

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.

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 students, 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

School social media passwords are kept securely by ICT Support.

Staff will ensure any posts are positive in nature and relevant to students, 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 students.

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

Staff will ensure the Executive Headteacher/ Headteacher has checked the content before anything is posted on social media. If staff wish for reminders to be posted for parents, e.g.,

returning slips for a school trip, staff will seek permission from the Executive Headteacher/ Headteacher before anything is posted.

If inappropriate content is accessed online, ICT Support should be notified. The Trust retains the right to monitor students' and staff members' internet usage in line with the Data and Cyber-security Breach Prevention and Management Plan.

The school's social media accounts will comply with site rules at all times, particularly with regards to the minimum age limit for use of the site. It will be noted that each networking site has its own rules which must be followed, ICT Support will induct staff to each new social media platform, providing them with the relevant training and information.

Personal accounts

Staff members will not access social media platforms during lesson times, but they are permitted to use social media during break times. Staff will avoid using social media in front of students.

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 Executive Headteacher/ Headteacher.

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

Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to students or parents – any contact with students' parents will be done through authorised school contact channels. 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.

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. 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.

No staff member will post any content online that is damaging to the school or any of its staff or students. Staff members will not post any information which could identify a student 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.

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.

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.

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

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

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 students when commenting on school social media sites, nor post comments concerning other students staff members, in accordance with the Social Media Code of Conduct for Parents.

Any parents that are seen to be breaching the guidance in this policy will be required to attend a meeting with the Executive Headteacher/ 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.

Student social media use

Students are not permitted to use the school's WiFi network to access any social media platforms unless prior permission has been sought from the Executive Headteacher/ Headteacher, and the online safety officer has ensured appropriate network security measures are applied. The Trust's Webfilters prevent students using the Trust's WiFi network to access any social media platforms.

Students will not attempt to 'friend', 'follow' or otherwise contact members of staff through their personal social media accounts. Where a student attempts to "friend" or 'follow' a staff member on their personal account, it will be reported to ICT Support.

Students will not post any content online which is damaging to the school or any of its staff or students and will not post anonymously or under an alias to evade the guidance given in this policy.

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

If inappropriate content is accessed online on school premises, it will be reported to ICT Support.

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

Online safety

Any disclosures made by students 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 Executive Headteacher/ 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 Executive Headteacher/ Headteacher it will be reported to the Chair of Governors.

Concerns regarding a student's online behaviour will be reported to the DSL, who will investigate any concerns with relevant staff members, e.g., the Executive Headteacher/ Headteacher or ICT Support and manage concerns in accordance with relevant policies depending on their nature, e.g., the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Executive Headteacher/ Headteacher will contact the police. The school will avoid unnecessarily criminalising students, 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 student having 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.

As part of the usual communication with parents, the school will reinforce the importance of students 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 sites they will be asked to access and who from the school, if anyone, they will be interacting with online.

Blocked content

In accordance with the Trust's Data and Cyber-security Breach Prevention and Management Plan, the ICT Services Manager will deploy and manage a webfilter 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

The online safety officer retains the right to monitor staff and student access to websites when using the school's network and on school-owned devices.

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

Access to inappropriate content is managed by ICT Support through the ICT Helpdesk.

Cyberbullying

Cyberbullying incidents are taken seriously at the Robert Carre Trust. Any reports of cyberbullying on social media platforms by students will be handled in accordance with the Anti-bullying Policy.

Cyberbullying against students 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 Abuse Against Staff Policy.

Training

The school recognises that early intervention can protect students who may be at risk of cyberbullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk students, teachers and support staff will receive training on social media as part of their new starter induction. Teachers and support staff will receive ongoing training as part of their development.

Students 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. Students 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, such as our Social Media Code of Conduct for Parents.

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

Recruitment

In line with current guidance the Trust reserves the right to carry out social media checks on potential new staff during the recruitment process.

Agreed by Trustees on 26 September 2023

Next Review Date: September 2024 (annually)