The Robert Carre Trust

Social Media Policy

Policy statement

We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to our ability to safeguard children and young people, protect confidential information and reputation, and can jeopardise our compliance with legal obligations. This could also be the case during off duty time.

Employees using social media are also potentially at risk of others misunderstanding the intent behind online communications or the blurring of professional boundaries between children and young people and their parents or carers. This policy, therefore, sets out the Robert Carre Trust's expectations regarding the use of social media.

To minimise these risks, to avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate business purposes, and that the use of personal devices does not have an adverse impact on our business, we expect employees to adhere to this policy.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

Who is covered by the policy?

This policy covers all employees working at all levels and grades. It also applies to consultants, contractors, casual and agency staff (collectively referred to as 'staff' in this policy). Trust staff responsible for consultants, contractors, casual or agency staff are to bring this policy to their attention.

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

Scope and purpose of the policy

This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, all other social networking sites, and all other internet postings, including blogs.

It applies to the use of social media for both business and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Breach of this policy may result in disciplinary action up to, and including, dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach.
Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Personnel responsible for implementing the policy

The Board has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Executive Headteacher/Head of School. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Executive Headteacher/Head of School.

All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Executive Headteacher/Head of School. Questions regarding the content or application of this policy should be directed to the Executive Headteacher/Head of School.

Compliance with related policies and agreements

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- breach our ICT Acceptable Use policy;
- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations they may have relating to confidentiality;
- breach our Staff Disciplinary policy;
- defame or disparage the Robert Carre Trust or its affiliates, governors, students, parents and carers, staff, business partners, suppliers, vendors or other stakeholders;
- harass or bully other staff in any way or breach our Anti-bullying policy;
- unlawfully discriminate against other staff or third parties or breach our Equal Opportunities policy;
- breach any other laws, such as the Data Protection Act and GDPR Regulations, or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the Robert Carre Trust and create legal liability for both the author of the reference and the Trust.

Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Personal use of social media

Personal use of social media is not permitted during working time or by means of our computers, networks and other IT resources and communications systems.

Monitoring

The contents of our IT resources and communications systems are our property. Whilst the Trust adheres to the requirements of the Data Protection Act, staff should not assume they have an automatic right to privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems including, but not limited to, social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

We will comply with the requirements of Data Protection Legislation (being (i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998) in the monitoring of our IT resources and communication systems Monitoring undertaken is in line with our Staff Privacy Notice which sets out how we will gather, process and hold personal data of individuals during their employment. Our GDPR Policy sets out how we will comply with Data Protection Legislation.

In line with the requirements of Data Protection Legislation, we may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice. Records will be kept in accordance with our Staff Privacy Notice and our Records Management Policy

Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the Trust.

For further information, please refer to the Trust's ICT Acceptable Use policy.

Business use of social media

If your duties require you to speak on behalf of the Trust in a social media environment, you must still seek approval for such communication from your manager or the Executive Headteacher/Head of School, who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the Trust for publication anywhere, including in any social media outlet, direct the inquiry to the Executive Headteacher's PA and do not respond without written approval.

The use of social media for business purposes is subject to the remainder of this policy.

Responsible use of social media

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely and in order to protect staff and the Trust.

Employees' use of social media can pose risks to our ability to safeguard children and young people, protect our confidential information and reputation, and can jeopardise our compliance with our legal obligations. This could also be the case during 'off duty' time.

Safeguarding children and young people:

- You should not communicate with students over social network sites, except for where there is a familial relationship[1], and should block communications from students. You should never knowingly communicate with students[1] in these forums or via personal email account.
- You should not interact with any ex-student[1] of the Trust who is under 18 on such sites.
- Communication with students should only be conducted through our usual channels. This communication should only ever be related to our business.

Staff who become aware of inappropriate posts or communications that breach these guidelines and that suggest a student might be at risk of harm should report their concerns to the Designated Safeguarding Lead.

Protecting our business reputation:

Staff must not post disparaging or defamatory statements about:

- our Trust;
- our students or their parents or carers;
- our Members, Trustees, Governors or staff;
- suppliers and vendors; and
- other affiliates and stakeholders,

Staff should also avoid social media communications that might be misconstrued in a way that could damage the Trust's reputation, even indirectly.

Staff should make it clear in social media postings that they are speaking on their own behalf. Write in the first person and use a personal email address when communicating via social media.

Staff are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by the masses, including the Trust itself, future employers and social acquaintances for a long time. Keep this in mind before you post content. Staff should also remember that once a comment/image has been shared, the poster loses control of the comment/image.

If you disclose your affiliation as an employee of our Trust, you must also state that your views do not represent those of your employer. For example, you could state, 'the views in this posting do not represent the views of my employer'. You should also ensure that your profile and any content you post are consistent with the professional image you present to students and colleagues.

Avoid posting comments about sensitive Trust related topics, such as our performance. Even if you make it clear that your views on such topics do not represent those of the Trust, your comments could still damage our reputation.

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with the Executive Headteacher/Head of School.

If you see content in social media that disparages or reflects poorly on the Trust or our stakeholders, you should either print out the content or save a screenshot of the post and contact the ICT Services Manager. All staff are responsible for protecting the Trust's reputation.

[1] Staff who have children or relatives who are students within a Trust school should give very careful consideration as to the professional risks associated with connecting with the child via social network pages/accounts that the child's peers may be able to access.

Respecting intellectual property and confidential information:

Staff should not do anything to jeopardise our confidential information and intellectual property through the use of social media.

In addition, staff should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for the Trust, as well as the individual author.

Do not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.

Respecting colleagues, students, parents and carers, governors and other stakeholders:

Do not post anything that your colleagues or our students, parents and carers, governors and other stakeholders would find offensive, including discriminatory comments, insults or obscenity.

Social Media Guidelines

There may be occasions where, for legitimate reasons, employees will need to post information on websites as part of their role. In all circumstances, except for ICT Support who are authorised to post items on the Trust's social media accounts or websites, authorisation from the Executive Headteacher/Head of School must be sought before proceeding.

Internet activities are not anonymous or secure and can, therefore, have an impact on the reputation of the Trust. For this reason we expect all employees who engage with social media on behalf of the Trust to understand and to follow these guidelines:

Your responsibility – whatever you write is ultimately your responsibility;

Ensure you are the expert – you are personally responsible for what you write, please ensure you only write and post comments about your areas of expertise/responsibility;

Where you are not the expert – if your engagement leads to areas outside of your expertise please take advice from the Executive Headteacher/Head of School before responding;

Transparency – it is imperative that when you are using social media as part of your job that you are transparent and honest about who you are and who you work for. Therefore, ensure you use your real name, identify that you work for the Trust and be clear about your role. Never hide behind anonymous or pseudonymous comments;

Be truthful – anything that you say must be true and not misleading. Any claims or statements you make must be capable of being substantiated and approved. What you publish will be around for a long time, so consider the content carefully and never guess what you think the correct answer may be;

The Trust's reputation – remember that by identifying yourself as a Trust employee, you are creating a perception about the Trust. It is, therefore, imperative you maintain high standards of English, spelling and grammar;

Confidentiality – be smart about protecting yourself, your privacy and the Trust's confidential information. What you publish is widely accessible so consider the content carefully and whether it is sensitive;

Made a mistake? – if you happen to make a mistake, admit it quickly. If you are posting to a blog, you can modify your earlier post as long as you make it clear that you have done so;

Monitoring – anything in the public domain is open to scrutiny and staff should be aware that designated Trust staff may monitor such material if a breach of this policy applies or is suspected. A member of SLT or other appropriate person may view communications with or without an employee's consent in certain circumstances, which includes cooperating with an external investigation that may take place by the Police or Social Services.

Enforcement

The Trust may require the removal of content published by employees that adversely affects the Trust community or puts the Trust at risk of legal action.

Any online communication published by employees that is illegal or in breach of data protection/confidentiality or deemed inappropriate for public exchange or causes damage to the Trust community's reputation is strictly forbidden.

Employees should be aware that without consent, the Trust may monitor or record communications where inappropriate activity involving children is suspected, or in other circumstances where there is reasonable suspicion that an offence is being, or likely to be committed. Any activity deemed to raise a safeguarding concern will be reported to the relevant authorities in accordance with statutory and legal duties. In such cases, where the activity involves, or is believed to involve, the use of school issued equipment the Trust would take possession of such equipment and retain for the relevant authorities to investigate.

Breaches of this policy may be regarded as misconduct, or even gross misconduct for a serious breach, and could lead to disciplinary action up to and including summary dismissal.

Examples of activities that may be regarded as gross misconduct include but are not limited to:

- Accessing or posting inappropriate or illegal content or images relating to children;
- Writing anything which is malicious, defamatory, untrue, hurtful, personal or otherwise offensive about the Trust community;
- Writing anything about the Trust community that is either a breach of confidential information or is likely to harm, lower or damage the reputation of the Trust community or adversely affect it;
- Posting any videos, photographs, or any other media which is inappropriate and/or does, or is likely to harm, lower or damage the reputation of the Trust community or adversely affect it.

Staff as victims of abuse/bullying via social media

The Trust recognises that staff themselves, despite adherence to this policy, may become the victims of online abuse via social media. Staff who suspect they are being targeted on social media by students and/or their parents and associates should not engage in a response via social media but should report the matter to the Executive Headteacher/Head of School at the earliest opportunity.

Students engaging in such activity will be dealt with through the normal disciplinary procedures. Where appropriate the matter will be referred to the relevant authorities. This policy will not preclude staff from seeking their own redress from the relevant authorities but seeks to assure staff that the Trust takes its responsibility for the welfare of its employees seriously and will do all within its jurisdiction to support the member of staff in pursuing appropriate action.

Where the perpetrator is a parent/carer or an associate, the Trust will seek to address the matter on behalf of the employee and/or support the employee in pursuing the intervention of the relevant authorities. Where appropriate the actions outlined in the policy relating to Vexatious Communications will ensue.

Associated Policies: Anti-Bullying

Code of Conduct
GDPR
ICT Acceptable Use
Safeguarding
Staff Disciplinary
Vexatious Communications

This policy is reviewed annually by the Robert Carre Trust. We will monitor the application and outcomes of this policy to ensure it is working effectively.

Agreed by SLT September 2018

Next Review Date: September 2019. (annually)