



**Social Media Policy**  
**September 2021**

## **Contents**

1. Introduction .....	2
2. Personal use of social media .....	2
3. Prohibited use .....	2
4. Business use of social media .....	3
5. Guidelines for responsible use of social media .....	3
6. Monitoring .....	3
7. Breach of this policy .....	4

## 1. Introduction

The aims of this policy are to:

- enable appropriate use of social networking sites in a safe and secure manner
- safeguard employees in their use of social networking sites and ensure they do not make themselves vulnerable
- minimise the risks to the Trust through use of social media

For the purposes of this policy, social media is any online platform or app that allows parties to communicate with each other or to share data in a public forum. This includes social forums such as Twitter, Facebook, Instagram, WhatsApp and LinkedIn. Social media also covers blogs, image-sharing and video websites such as YouTube.

Employees should be aware there are many more examples of social media than can be listed here and this is a constantly changing area. **Employees must follow these guidelines in relation to any social media platform that they use.**

This policy applies to use of social media for business purposes as well as personal use that may affect the Trust in any way. It covers all employees, consultants, volunteers and agency workers.

This policy does not form part of any employee's contract of employment and it may be amended at any time. The Trust may also vary this policy as appropriate in any case.

## 2. Personal use of social media

Employees must limit their personal use of social media on their own equipment to rest breaks such as lunch or break times. The use of personal devices must be discreet and not in the **presence of pupils under any circumstances.** Personal use may not interfere with employment responsibilities or productivity and comply with this policy.

## 3. Prohibited use

Employees must not abuse their position of trust with pupils including, but not limited to:

- accepting any current pupils, or former pupil under the age of 18, as friends, or requesting such friendships
- communicating personally with pupils
- posting photographs of pupils on sites not owned by the Trust; or
- commenting about or naming pupils

The employee must avoid making any social media communications that could damage the Trust's interests or reputation, even indirectly.

The employee must not use social media to:

- defame or disparage the Trust, its employees or any third party
- harass, bully or unlawfully discriminate against staff or third parties
- make false or misleading statements
- impersonate colleagues or third parties

The employee must not express opinions on the Trust's behalf via social media, unless expressly authorised to do so and through the appropriate approved social media channels.

The employee must not post comments about sensitive school-related topics, such as the Trust's performance, internal disputes involving pupils, parents or employees and must not do anything to jeopardise confidential information particularly with regards to pupils and other employees. The employee must not include the Trust's logo or other trademarks in any social media posting, unless expressly authorised to do so.

Employees should never provide professional references on behalf of the Trust for other individuals without the express authority of the Headteacher/ Executive Headteacher including on social or professional networking sites. Such references, positive and negative, can be attributed to the Trust and create legal liability for both the author of the reference and the Trust.

Social media should never be used in a way that breaches any other Trust policies. If an internet post would breach any policy/ procedure in another forum, it will also breach them in an online forum.

#### **4. Business use of social media**

If an employee is contacted for comments about the Trust for publication anywhere, including in any social media outlet, the enquiry should be directed to the Line Manager/Headteacher and the employee should not respond without written approval.

#### **5. Guidelines for responsible use of social media**

The employee should make it clear in social media postings that the employee is speaking on the employee's own behalf.

Employees should be respectful to others when making any statement on social media and be aware that the employee is personally responsible for all communications which will be published on the internet for anyone to see. Employees should ensure that they use privacy and access settings whilst being aware that they cannot control the use of their postings by others.

The employee should also ensure any content they post on social media are consistent with the professional image the employee presents to colleagues, pupils and parents.

If the employee is uncertain or concerned about the appropriateness of any statement or posting, they are advised to refrain from posting it until they have discussed it with their manager.

If the employee becomes aware of social media content that disparages or reflects poorly on the Trust, the employee should contact their Line Manager or the Headteacher.

#### **6. Monitoring**

The Trust reserves the right to monitor, intercept and review, without further notice, employee activities using school IT resources and communications systems, including but not limited to social media postings and activities, to ensure that Trust rules are being complied with and for legitimate school purposes.

For further information, please refer to the eSafety and data security policy.

## Governors

Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare. Policies should be in place for staff which include a **staff behaviour policy** (sometimes called the code of conduct) which should, amongst other things, include: acceptable use of technologies (including the use of mobile devices), staff/pupil relationships and communications including the use of social media, (Keeping Children Safe in Education 2021).

**All** staff should be aware of systems within their school or college which support safeguarding and these should be explained to them as part of staff induction.

This should include the:

- child protection policy, which should amongst other things also include the policy and procedures to deal with peer on peer abuse;
- behaviour policy (which should include measures to prevent bullying, including cyberbullying, prejudice-based and discriminatory bullying);<sup>6</sup>
- staff behaviour policy (sometimes called a code of conduct);
- safeguarding response to children who go missing from education; and role of the designated safeguarding lead (including the identity of the designated safeguarding lead and any deputies). (Keeping Children Safe in Education 2021).

All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins and staff meetings), as required, and at least annually, to provide them with relevant skills and knowledge to safeguard children effectively. (Keeping Children Safe in Education 2021).

At Roebuck Academy all members of staff are provided with information about acceptable use of technologies, staff/pupil relationships and the use of social media as part of induction. At Roebuck Academy all staff are involved in the development and construction of policies to promote ownership and understanding. This involves including staff in development via discussions at staff meetings and reviewing policies with staff working groups.

## 7. Breach of this policy

Breach of this policy may result in disciplinary action up to and including dismissal.

The employee may be required to remove any social media content that the Trust consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

The Trust considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- been using social media when they should be working
- acted in a way that is in breach of the rules set out in this policy