

Policy and Procedure: Social Media/E-Safety

Date of Board Approval: April 2018

Review date: February 2019



1. Policy Statement

- 1.1 The Academy 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 the safeguarding of our pupils, our confidential information, reputation, and can jeopardise our compliance with legal obligations.
- 1.2 To minimise these risks and to ensure that our IT resources and communications systems are used only for appropriate purposes, we expect employees to adhere to this policy.
- 1.3 This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. Who is covered by the Policy?

- 2.1 This policy covers all individuals working at all levels and grades, including members of the senior leadership team, teachers, support staff, all employees, consultants, contractors, trainees, home workers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as "**staff**" in this policy).
- 2.2 Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

3. Scope and Purpose of the Policy

- 3.1 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.
- 3.2 It applies to the use of social media for both work 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.
- 3.3 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. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

3.4 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.

4. Personnel Responsible for implementation of the Policy

4.1 The Board of Trustees have overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Principal. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with all senior and middle managers.

4.2 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.

4.3 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 line manager. Questions regarding the content or application of this policy should be directed to a senior member of staff.

5. Compliance with related Policies and Agreements

5.1 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 Policy
- breach our Child Protection Policy
- breach our obligations with respect to the rules of relevant regulatory bodies
- breach any obligations they may have relating to confidentiality
- breach our Disciplinary Rules
- defame or disparage the Academy
- harass or bully other staff in any way
- unlawfully discriminate against other staff or third parties
- breach our Data Protection Policy (for example, never disclose personal information about a colleague online)
- breach any other laws 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)

5.2 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 Academy and create legal liability for both the author of the reference and the Academy.

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

6. Personal Use of Social Media

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems.

7. Contact with Pupils and/or parents/carers

- 7.1 You must not contact any pupil and/or parent/carer on any form of social media. If a pupil and/or parent/carer contacts you on social media, you must immediately notify the Principal. You must not enter into any correspondence with a pupil and/or parent/carer on social media.
- 7.2 Staff should refrain from contacting/entering into correspondence with previous pupils and/or parents/carers of the Academy on any form of social media, particularly where such contact could jeopardise the reputation of the Academy and/or member of staff.
- 7.3 If your duties require you to contact pupils and/or parents/carers by email on behalf of the Academy, you must ensure the content is professional and consistent with written communication sent by the Academy.
- 7.4 All staff have a duty towards safeguarding our pupils' wellbeing. Therefore, if you become aware of any act which may breach any of the terms of our Child Protection Policy on any form of social media, you must immediately report the matter to the Principal.

8. Monitoring

- 8.1 The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of 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.
- 8.2 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.
- 8.3 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.
- 8.4 Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the Academy.

9. The Academy use of Social Media

- 9.1 If your duties require you to speak on behalf of the Academy in a social media environment, you must still seek approval for such communication from the Principal, who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

9.2 Likewise, if you are contacted for comments about the Academy for publication anywhere, including in any social media outlet, direct the inquiry to the Principal and do not respond without written approval.

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

10. Responsible use of Social Media

10.1 The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

10.2 ***You should be aware that any comments made via the use of social media are subject to exactly the same legal rules as any other written comments. As such both you and the Academy may be at risk of legal proceedings if the comments breach the legal rules, in particular those relating to any breach of confidentiality or any disparaging or defamatory statements etc.***

10.3 Protecting our reputation:

- Staff must not post disparaging or defamatory statements about:
 - the Academy;
 - our pupils and/or parents/carers;
 - our employees;
 - our trustees, and/or
 - other affiliates and stakeholders.
- staff should avoid social media communications that might be misconstrued in a way that could damage our 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 e-mail 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 Academy itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.
- You must not disclose your affiliation as an employee of our Academy. You should also ensure that your profile and any content you post are consistent with the professional image you present to pupils and colleagues.
- You must not post comments about sensitive work-related topics, such as our performance. Even if you make it clear that your views on such topics do not represent those of the Academy, 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 Principal.

- If you see content in social media that disparages or reflects poorly on the Academy or our stakeholders, you should contact the Principal. All staff are responsible for protecting our reputation.

10.4 Respecting confidential information:

- Staff should not do anything to jeopardise our confidential information through the use of social media.
- Do not use our logos or post any of our confidential or proprietary information without prior written permission.
- You are not permitted to add pupils', parents and/or carer's contacts made during the course of your employment to personal social networking accounts, such as Facebook accounts or LinkedIn accounts.

10.5 Respecting colleagues, pupils, parents/carers, trustees and partners:

- Do not post anything that your colleagues or our pupils, parents/carers, trustees, partners would find offensive, including discriminatory comments, insults or obscenity.
- Do not post anything related to your colleagues or our pupils, parents, carers, trustees, partners or other stakeholders without their written permission.

11. Monitoring and Review of this Policy

11.1 The Principal in conjunction with the Board of Trustees shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

11.2 The Principal and Board of Trustees have responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

11.3 Staff are invited to comment on this policy and suggest ways in which it might be improved by contacting his/her line manager or a member of the senior team.