essa

Foundation
Academies Trust

SOCIAL MEDIA POLICY

Policy updated by: Stacey O’Connor November 2018

Date Reviewed: November 2019 by Stacey O’Connor (Essa Academy DSL)

Next Review: April 2021

Microsoft Office User

Social Media Policy

1.0 Policy Statement

1.1 The Academy recognises that the internet provides unique opportunities to participate in interactive discussions, engage with the wider community, and share information on particular topics using a wide variety of social media, such as Instagram, Facebook, Twitter and blogs. However, employees use of social media can pose risks to the Academy's confidential and proprietary information, reputation and can jeopardise compliance with legal obligations.

1.2 To minimise these risks, to avoid loss of productivity and to ensure that the Academy's IT resources and communications systems are used only for appropriate business purposes, the Academy expects employees to adhere to this policy, which outlines staff responsibilities when accessing and using social media websites.

1.3 This policy does not form part of any employees contract of employment and may, after consultation with the recognised trade unions, be amended at any time by the Academy.

1.4 Nothing in this Policy is intended to restrict or undermine the right to academic freedom.

2.0 Who is covered by the policy

2.1 This policy covers all individuals working at all levels and grades, including full time, part-time employees, fixed-term, consultants, contractors, casual, agency staff and volunteers (collectively referred to as **staff** in this policy).

2.2 Third parties who have access to the Academy's electronic communication systems and equipment are also required to comply with this policy.

3.0 Scope and purpose of the policy

3.1 This policy deals with the use of all forms of social media, including but not limited to, Instagram, Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs. The Academy has a separate policy regarding acceptable use of IT systems more generally and all staff should ensure that they read and understand that policy as well as this social media policy.

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

3.3 The purpose of this policy is to encourage good practice; to protect the Academy, its staff and students; to clarify where and how existing policies and procedures apply to social media and to promote effective and innovative use of social media as part of the Academy's activities.

3.4 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 the Academy's 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 an investigation, which may involve handing over relevant passwords and login details. The Academy also reserves the right to suspend internet or computer access where it deems it necessary during an investigation. When considering any potential breach of this policy, the Academy will consider the context of any social media posting.

3.5 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.

4.0 Responsible use of social media

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

4.2 Protecting the Academy's business reputation:

(a) Staff must not post disparaging or defamatory statements about:

(i) the Academy;

(ii) its clients;

(iii) its employees;

(iv) its students;

(v) its suppliers and vendors; and

(vi) other affiliates and stakeholders,

but staff should also avoid social media communications that might be misconstrued in a way that could damage the Academy's business reputation, even indirectly.

(b) Unless expressly authorised to speak on behalf of the Academy, either using an Academy social media account or otherwise, in accordance with section 8, staff should make it clear in social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal e-mail address when communicating via social media.

(c) Staff are personally responsible for what they communicate in social media. Staff should remember that what they publish might be available to be read by a wider audience (including the Academy itself, future employers and social acquaintances) for a long time. Staff should keep this in mind before posting content.

(d) If employees disclose their affiliation as an employee of the Academy, unless expressly authorised to speak on behalf of the Academy, either using n Academy social media account or otherwise, in accordance with section 8, they must also state that their views do not represent those of their employer. For example, employees could state, "the views in this posting do not represent the views of my employer". Employees should also ensure that their profile and any content they post are consistent with the professional image they present to students, clients, and colleagues.

(e) Staff should avoid posting comments about sensitive business-related topics, such as the performance or topics circulating in the press. Even if staff make it clear that their views on such topics do not represent those of the Academy, their comments could still damage the reputation or breach confidentiality obligations.

(f) If staff are uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they have discussed it with the E-safety lead or the Principal.

(g) If staff see content in social media that disparages or reflects poorly on the Academy or its stakeholders, they should contact the E-safety lead or the Principal. All staff are responsible for protecting the business reputation.

(h) Staff should use Academy e-mail addresses for the conduct of Academy business via social media. Use of private e-mail addresses for the Academy business is prohibited.

4.3 Respecting intellectual property and confidential information:

(a) Staff should not do anything to jeopardise the Academy's valuable trade secrets and other confidential information and intellectual property through the use of social media.

(b) In addition, staff should avoid misappropriating or infringing the intellectual property of other organisations and individuals, which can create liability for the Academy, as well as the individual author.

(c) Staff must not use the Academy or Trust logos, brand names, slogans or other trademarks in any social media post, or post any confidential information without prior written permission from the Principal.

(d) To protect themselves and the Academy against liability for copyright infringement, where appropriate, staff should reference sources of particular information they post or upload and cite them accurately. If staff have any questions about whether a particular post or upload might violate anyone's copyright or trademark, they should seek advice before making the communication.

4.4 Respecting colleagues, students, clients, partners and suppliers:

(a) Staff must not post anything relating to their colleagues or the Academy's students, clients, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenities.

(b) Staff must not post anything (e.g. comments or images) related to their colleagues, or the Academy's students, clients, patients, business partners, suppliers, vendors or other stakeholders without their (/an owner's) prior written permission.

5.0 Personnel responsible for implementing the policy

5.1 The Academy has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Head of IT Infrastructure Services.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the E-Safety lead (Stacey O'Connor – DSL).

5.2 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.

5.3 All staff are responsible for the effectiveness 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 Principal or Human Resources.

6.0 Compliance with related policies and agreements

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

(a) breach the IT Acceptable Use Policy;

(b) breach any obligations with respect to the rules of relevant regulatory bodies;

(c) breach any obligations employees may have relating to confidentiality;

(d) breach the Academy's Disciplinary Procedure;

(e) defame or disparage the Academy or its affiliates, clients, students, business partners, suppliers, or other stakeholders;

(f) breach the E Safety Policy;

(g) unlawfully discriminate against other staff or third parties or breach the Equal Opportunities Policy;

(h) breach the Data Protection Act or the Data Protection Policy (for example, never disclose personal information online); or

(i) breach any other laws or ethical standards (for example, social media should never be used in a false or misleading way, such as by employees claiming to be someone other than themselves or by making misleading statements).

6.2 Unless expressly authorised to do so in writing by the Principal, 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.

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

7.0 Personal use of social media

7.1 The use social media for personal activities should never take place during working hours or using Academy IT resources and systems. All social media sites are blocked from Academy IT equipment, however limited members of staff may have access to social media if they have rights to oversee the Academy's social media sights. Therefore, staff that have this in place should not allow their access abilities to use their own social media sites or for their own use in any way.

8.0 Business use of social media

8.1 If an employee wishes to create an Academy social media account, prior written approval must be sought from the Principal. On this page there must be no logos or links to the Academy.

8.2 If an employee's duties require them to speak on behalf of the Academy in a social media environment, approval must be sought for such communication from the Principal, who may advise them to undergo training before they do so and impose certain requirements and restrictions with regard to social media activities. The only exception to this is when the employee has previously been expressly authorised to speak on behalf of the Academy in a social media environment.

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

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

9.0 Monitoring

9.1 The contents of the IT resources and communications systems are the Academy's 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 the Academy's electronic information and communications systems.

9.2 The Academy reserves the right to monitor, intercept and review, without further notice, staff activities using its IT resources and communications 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.

9.3 The Academy 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.

9.4 Staff should not use the IT resources and communications systems for any matter that they wish to be kept private or confidential from the Academy.

9.5 Staff should never communicate with students or previous students of the Academy. If a student does contact them they should inform the safeguarding officer to report this. In exceptional circumstances if members of staff have relatives who are students or previous students of the Academy the member of staff should alert the Principal to this so that they are aware. Although the academy does not advise this to safeguard ourselves as it puts staff in a vulnerable position.