The de Ferrers Trust

SOCIAL MEDIA POLICY

Author:	Mrs J Harrison, HR Manager at The de Ferrers Academy
Approval needed by:	Board of Directors
Consultation with Unions (date):	30 November 2015
Adopted (date):	8 December 2015
Date of next review:	December 2017

Contents

1	Introduction	2
2	Scope and purpose of the policy	2
3	Personnel responsible for implementing the policy	2
4	Compliance with related policies and agreements	3
5	Personal use of social media	3
6	Monitoring	3
7	School use of social media	4
8	Recruitment	4
9	Responsible use of social media	4

1 Introduction

1.1 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 confidential and proprietary information, and reputation, and can jeopardise our compliance with legal obligations.

1.2 To minimise these risks, to avoid loss of productivity 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 The ICT Security Policy has a set of guidelines to refer to on Social Media and the use of mobile telephones for your use in conjunction with this policy.

2 Scope and purpose of the policy

2.1 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.

2.2 It applies to the use of social media for both work and personal purposes, whether during academy 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.

2.3 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.

2.4 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.

3 Personnel responsible for implementing the policy

3.1 The Board of Directors has 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 the Principal in conjunction with the HR Team.

3.2 All managers or heads of departments 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.

3.3 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 HR Team. Questions regarding the content or application of this policy should be directed to the HR Team in the first instance

.

4 Compliance with related policies and agreements

4.1 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:

(a) breach our ICT Security Policy;

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

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

(d) breach our Disciplinary Rules;

(e) defame or disparage the Trust or its academies, affiliates, students, parents, business partners, suppliers, or other stakeholders;

(f) harass or bully other staff in any way OR breach our Harassment and Bullying Policy;

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

(h) breach our Data Protection Policy (for example, never disclose personal information about a colleague online);

(i) 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).

4.2 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 Trust and create legal liability for both the author of the reference and the Trust.

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

5 Personal use of social media

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

6 Monitoring

6.1 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.

6.2 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 trust 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.

6.3 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.

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

6.5 For further information, please refer to our ICT Security Policy.

7 Academy use of social media

7.1 If your duties require you to speak on behalf of the Trust or an Academy within it, 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.

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

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

8 Recruitment

8.1 We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

9 Responsible use of social media

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

9.2 Protecting our Trust's reputation:

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

(i) our academies;

(ii) their colleagues;

(iii) students or their parents;

(iv) suppliers and vendors; and

(v) other affiliates and stakeholders,

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

(b) 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.

(c) 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.

(d) If you disclose your affiliation as an employee of our academies, 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 pupils, parents and colleagues.

(e) Avoid posting comments about sensitive academy-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 or your Academy, your comments could still damage our reputation.

(f) 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.

(g) If you see content in social media that disparages or reflects poorly on our trust or our academies, you should contact the Principal. All staff are responsible for protecting our trust's and the individual academies' reputations.

9.3 Respecting intellectual property and confidential information:

(a) Staff should not do anything to jeopardise our 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 schools and individuals, which can create liability for the Trust, as well as the individual author.

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

(d) To protect yourself and the Trust against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Principal before making the communication.

(e) You are not permitted to add students to personal social networking accounts, such as Facebook accounts or LinkedIn accounts.

(f) Whilst the Trust appreciates the nature of relationships with friends who may in turn be parents of students at the academies, you are not permitted to bring the academies into disrepute on personal social networking accounts, such as Facebook accounts or LinkedIn accounts.

9.4 Respecting colleagues, students, partners and suppliers:

(a) Do not post anything that your colleagues or our students, parents, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.

(b) Do not post anything related to your colleagues or our students, parents, business partners, suppliers, vendors or other stakeholders without their written permission.