LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

SOCIAL MEDIA POLICY

CONTENTS

1.0 Introduction

1.1 The Council recognises 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, staff use of social media can pose risks to the Council's confidential and proprietary information, and reputation, and can jeopardise the Council's compliance with legal obligations.

1.2 To minimise these risks, to avoid loss of productivity and to ensure that the Council's IT resources and communications systems are used only for appropriate business purposes, we expect staff to adhere to this policy.

1.3 This policy does not form part of staff contracts of employment and it may be amended at any time.

2.0 Who is covered by the Policy?

2.1 This policy covers all individuals working at all levels and grades in the Council, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff (collectively referred to as staff in this policy).

2.2 Third parties who have access to the Council'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 Facebook, LinkedIn, Twitter, You Tube, 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 Council business and personal purposes, whether or not during office hours or otherwise. The policy applies regardless of whether or not the social media is accessed using the Council's 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 the Council'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 the Council's investigation.

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.

4.0 Compliance with Related Policies and Agreements

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

(a) breach the Council's Information Management and Security Policy;

(b) breach the Council's Disciplinary Rules;

(c) harass or bully other staff in any way;

(d) unlawfully discriminate against other staff or third parties;

(e) breach the Council's Data protection policy (for example, never disclose personal information about a colleague online);

(f) 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 Council and create legal liability for both the author of the reference and the organisation.

4.3 Staff who breach any of the above policies will be subject to disciplinary action, up to and including dismissal.

5.0. Personal use of Social Media

5.1 Personal use of social media is never permitted during working time.

5.2 We recognise that Staff occasionally may desire to use social media for personal activities at the office or by means of the Council's computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not take place during working time. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the Council's business are also prohibited.

5.3 The above arrangements apply equally to the use of privately owned Personal Electronic Devices (Mobile phones, Laptops, Tablets, Smart phones etc) as they do to Council owned equipment.

Note: The times when occasional use is authorised are; during lunchtime; before or after the working day or when "logged out" of the flexitime system.

6.0 Responsible Use of Social Media

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

6.1.1 **Protecting the Council's reputation:**

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

(i) the Council's organisation;

(ii) the Council's elected Members and employees;

(iii) the Council's service users;

(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 Council'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 Council 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 the Council, you must also state that your views do not represent those of the Council. For example, you could state, "the views in this posting do not represent the views of Lancaster City Council". You

should also ensure that your profile and any content you post are consistent with the professional image you present to service users and colleagues.

(e) Avoid posting comments about sensitive Council business. Even if you make it clear that your views on such topics do not represent those of the Council, your comments could still damage the Council's 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 your manager.

(g) If you see content in social media that disparages or reflects poorly on the Council or the Council's stakeholders, you should contact your manager. All staff are responsible for protecting the Council's business reputation.

6.1.2 **Respecting intellectual property and confidential information:**

(a) Staff should not do anything to jeopardise the Council's 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 companies and individuals, which can create liability for the Council, as well as the individual author.

(c) Do not use the Council's logos, or post any of the Council's confidential or proprietary information without prior written permission.

6.1.3 The contact details of business contacts made during the course of your employment are regarded as the Council's confidential information, and as such you will be required to delete all such details from your personal social networking accounts, such as Facebook accounts or LinkedIn accounts, on termination of employment.

6.1.4 **Respecting colleagues, elected Members, clients, partners and suppliers:**

(a) Do not post anything that your colleagues or the Council's elected Members, service users, business partners, suppliers, vendors or other stakeholders might find offensive, including discriminatory comments, insults or obscenity.

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

7.0 Monitoring

7.1 As with any Internet and e-mail use (including personal e-mail), the use of social media sites may be monitored or recorded by the Council at any time without notice or consent for the following purposes only:

- **To establish the existence of facts relevant to Council business**
  e.g. keeping records of transactions and other communications in cases where it is necessary or desirable to know the specific facts of the conversation.

- **To ascertain compliance with regulatory or self-regulatory practices or procedures relevant to Council business**

e.g. monitoring as a means to check that the Council is complying with regulatory or self-regulatory rules or guidelines.

- **To ascertain or demonstrate standards which are or ought to be received by persons using the telecoms system**
  e.g. monitoring for purposes of quality control or staff training.

- **To prevent or detect crime**
  e.g. monitoring or recording to detect fraud or corruption.

- **To investigate or detect the unauthorised use of the telecoms systems**
  e.g. monitoring to ensure that users do not breach Council rules regarding use of the telecoms systems.

- **To ensure the effective operation of the system**
  e.g. monitoring for viruses or other threats to the system; automated processes such as caching or load distribution.

7.2 The Council may also monitor (but not record) communications without notice or consent:

- **To check whether communications are relevant to Council business**
  e.g. checking e-mail accounts to access Council business communications in staff absence.

7.3 The Council, however, will not use personal information collected through monitoring for purposes other than for which the monitoring was undertaken unless the information is such that no reasonable Council or employer could ignore it i.e. it reveals criminal activity or gross misconduct.

7.4 Unless such monitoring would be ineffective and the circumstances justify the additional intrusion, the Council will limit monitoring to traffic data rather than the contents of communications and undertake spot checks or audit rather than continuous monitoring.

7.5 If the traffic record alone is not sufficient to achieve the business purpose use, the Council will ensure that any further monitoring is, as far as possible, limited and targeted.

7.6 Wherever possible the Council will restrict the monitoring of e-mails sent to specific users to messages the employee has received and chosen to retain rather than deleted.

8.0 Other related documents

The Council though it's Information Management Group, has developed a range of policies. This policy should be read in conjunction with any existing policies and protocols which may be amended from time to time. These documents can be accessed via the council intranet "ELSIE".