CEREDIGION

Social Media Policy

Author: Corporate HR

Cabinet Approval: 26 April 2016

Ceredigion County Council

Social Media Policy

1 INTRODUCTION

It is recognised that staff, like other members of the population, have a right to participate in social networking on websites including Facebook, Twitter, My Space, You Tube, LinkedIn.

The Council recognises the right to freedom of speech of its employees. Employees should recognise that this must be appropriate and not used as a substitute for following the correct Council policies, as detailed in Paragraph 2 below.

2 RELATED POLICIES AND DOCUMENTS

This policy should be read in conjunction with the following Council documents:

(i) The Code of Conduct
(ii) Information Security Policy
(iii) Disciplinary Policy
(iv) Grievance Procedure
(v) Whistleblowing Policy
(vi) Political Restrictions on Local Government Employees Policy
(vii) Social Media Editorial and Administration Policy (only relevant to staff responsible for Ceredigion County Council related social media pages)
(viii) Employee Handbook

3 SCOPE

3.1 This Policy applies to all Ceredigion County Council employees. This policy applies to the use of any social media applications which includes Facebook (social networking), Twitter (microblog), YouTube (video sharing), Flickr (image sharing) Instagram (image sharing). There are many more examples of social media than are listed here and it is recognised that this is a constantly changing area.

3.2 This policy also covers personal blogs, any posts you might make on other blogs, and to all online forums and noticeboards.

4 AIMS & OBJECTIVES

4.1 This policy sets out the principles to adhere to and offers guidelines relating to the use of social networking and other websites in order to:

- protect staff
- protect the Council
- prevent misuse
- protect the citizens of Ceredigion

4.2 The Policy aims to ensure that all employees are aware that failure to follow these guidelines could lead to disciplinary action under the Council's Disciplinary Policy and in more serious cases could be considered gross misconduct which may lead to dismissal

5 DUTIES AND RESPONSIBILITIES

5.1 The personal use of Council resources for social media must be reasonable and in accordance with Paragraph 6 of the Council Information Security Policy, namely:

"Personal usage is defined as usage of Council resources that is not directly associated with the performance of a user's official Council duties or job description. The Council shall reserve the right to introduce access controls that limit the extent of personal usage.

*Personal usage is only permitted where **all** the following apply:*

- *such use is of a private nature, not for financial gain and does not contravene any other Council policies;*
- *such use does not incur costs to the Council;*
- *such use does not disrupt the official business of the Council;*
- *such use must not involve anything that promotes illegal, sexual, or other activities that contravenes the Council's policies"*

5.2 Employees must be aware of their association with the Council when using social media. If they identify themselves or are identifiable as a Council employee, they should ensure that their profile and any related content is consistent with how they would wish to present themselves to colleagues, councillors, service users and members of the public.

5.3 Employees should make it clear that any posts reflect their opinions and they are not speaking on behalf of the Council.

5.4 Staff must be aware that any comments they make on social media outside of working hours may have implications on their contractual obligations to the Council. Such comments may also be the subject of a whistleblowing incident.

5.5 Staff must be aware that inappropriate or ill-considered use of social media has the potential to damage the reputation of themselves as individuals and/or the Council. Bringing the Council into disrepute may result in disciplinary action being taken.

5.6 During work time employees may only access and view pages from allowed social media sites which are required in their role. Use of sites must be justifiable and approved by their line manager in advance of accessing such sites.

6 SAFEGUARDING VULNERABLE ADULTS AND CHILDREN

6.1 A number of roles in the Council are involved in a safeguarding environment of children and vulnerable adults.

6.2 It is recognised that there are potential risks to children and vulnerable adults using social media and social networking sites. These risks include cyber bullying, grooming and potential abuse, identity theft and exposure to inappropriate content.

6.3 Staff in a safeguarding environment must recognise the sensitivity inherent in their roles and before engaging in any social media activity they should consider if their actions could create any potential safeguarding concerns.

7 POLITICALLY RESTRICTED POSTS

Employees in politically restricted posts as defined by the Council's Political Restrictions on Local Government Employees policy are reminded that the restrictions imposed by the policy apply equally to social media.

8 LINE MANAGERS

8.1 Line managers are responsible for ensuring that those in their team understand the requirements of this policy.

8.2 Line managers are expected to deal with concerns or issues raised by their staff in relation to social media usage or content by using, if appropriate, the relevant Council policy, for example disciplinary policy or grievance policy.

8.3 HR Officers are responsible for advising and supporting line managers in the application of this policy.

Appendix 1

Guidance for Council staff

The open nature of the Internet means that social networking sites can leave Council staff vulnerable if they fail to observe a few simple precautions. The below guidelines are intended as general advice on how to avoid compromising your professional position and reputation.

Privacy

- To ensure that your Facebook account does not compromise your professional position you should ensure that your privacy settings are set correctly. Where appropriate the recommended security level is for your settings to reflect 'Friends only'
- Always make sure that you log out of social media after using it, particularly when using a machine that is shared with other people. Your account can be hijacked by others if you remain logged in, even if you close your browser.

Conduct on social networking sites

- Do not make derogatory remarks about the Council, Council Members or your colleagues. If you wish to make a legitimate complaint the appropriate Council policies and/or channels should be used.
- Do not make any remarks about Council service users or customers
- Do not make any remarks about Council suppliers
- Do not publish any information which is confidential to the Council
- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them to have the material removed.
- Remember that what you publish will be in the public domain for a long time and may be shared widely without your consent.
- Consider the impact of what you publish upon your colleagues and members of the public.
- It may be possible for members of the public to access your profile and could, if they find the information and/or images it contains offensive, complain to the Council.
- If you have any concerns about information on your social networking site, or if you are the victim of cyberbullying, you should inform your Line Manager immediately.
- If you see potentially illegal/abusive content or activity, including child sexual abusive images and online grooming your should immediately inform your Service's Designated Safeguarding Officer.
- If you have any concerns about images or comments on social media you should inform your Line Manager immediately.
- Do not publish your date of birth and home address on Facebook.
- Do not use your work contact details as part of your personal profile
- Do not use your personal profile in any way for official Council business
- Ensure that any comments and/or images you post are not defamatory or in breach of copyright legislation.

- Unless they are family friends do not accept friend requests from children under the age of 18.
- Consider the implications of accepting friend requests from colleagues and whether your privacy settings need to be amended.
- Do not accept friend requests from members of the public where the primary relationship is through your work
- Where a child or vulnerable adult may be in immediate danger you should always dial 999 for police assistance.

Additional Safeguarding Guidance

- Do not ask pupils or service users to divulge any personal details that may help identify them as children or vulnerable adults and their location. These details will include home address, school and mobile number.
- Do not upload images of children and vulnerable adults due to the potential for:
  (a) tagging of children/vulnerable adults thus identifying them at a location and allowing the opportunity for abusers to identify and locate them on social media sites;
  (b) personal intimidation by posting derogatory, abusive and threatening comments
  (c) cyber bullying
- Before posting consider whether any photographs, images or text are appropriate and if they could create any potential safeguarding concerns
- Do not accept friend requests from pupils (or their parents) or vulnerable adult service users that you work with.