Social Media Guidance

Reference:	HRSM1
Version No:	D3
Issue Date:	December 2011

Document Control

Document Ref:	HRSM1	**Date Created:**	December 2011
Version:	D3	**Date Modified:**	
Revision due			
Author:	Katie Penlington	**Sign & Date:**	
Head of Service:	Robert O'Reilly	**Sign & Date:**	
Equality Impact Assessment: (EIA)	Date undertaken:		
	Issues (if any):		

Change History

Version	Date	Description	Change ID
D3	December 2011	Social Media Guidance	

Related Documents

Reference	Title	Tier
	ICT Policy	
	Code of Conduct	
	Disciplinary Procedure	

West Berkshire COUNCIL

Contents

1. Purpose

1.1. The purpose of this document is to provide guidance on the appropriate use of social media in order to:

1.1.1. Ensure that the reputation or credibility of the Council is not adversely affected.

1.1.2. Ensure that the Council is not subject to legal challenge as a result of material posted on social networking sites e.g. data protection, discrimination and other sensitive information.

1.1.3. Safeguard the privacy of service users.

2. Applicability

2.1. This guidance applies to all employees working for the Council, including those working from home or at non-Council locations.

2.2. Other persons who should have regard to this guidance include elected members, consultants, agency staff, volunteers and contractors working for the Council, external organisations working with the Council, whilst engaged on Council business.

2.3. It is the responsibility of all those stated above to familiarise themselves with and adhere to this guidance.

2.4. This guidance/policy should be read in conjunction with the Council's ICT Policy, the Code of Conduct for Officers and Members and the Disciplinary Rules.

2.5. This guidance is primarily concerned with personal use of social media. Where social media sites are used as part of service delivery, any service specific rules that apply should also be followed.

3. Roles and Responsibilities

3.1. Those listed above are responsible for familiarising themselves with, and ensuring that they comply with this standard and ensuring that their use of social media, whether at work or in their own time work, **does not**:

- Adversely affect the Council or its business
- Damage the Council's reputation or credibility
- Breach any Council policies
- Put service users or colleagues at risk

3.2. Failure to follow this guidance, even where the use of social media has occurred outside work, may lead to action being taken against employees under the Council's disciplinary procedure. Relevant action will be taken against non-employees.

4. The reputation of the Council

4.1. Maintaining credibility with the public is very important to the Council. It is important that the reputation of the Council is not damaged by the actions of employees either at work, or through their actions outside of work.

4.2. The Council's Code of Conduct for Employees states;

'The public is entitled to expect the highest standards of integrity from local government employees and to know that decisions and actions taken are fair and impartial. Public confidence is shaken if there is the least suspicion, however ill founded, that there has been improper conduct or that decisions and/or actions have been influenced by improper motives or pressures. Councils are expected to provide clear guidance to their employees on what is acceptable conduct and what is not.'

4.3. The WBC Code of Conduct for Members states;

'You must not conduct yourself in a manner which could reasonably be regarded as bringing your office or authority into disrepute.'

4.4. The Disciplinary Rules give the following as examples of gross misconduct:

'Omission or conduct liable to lead to serious loss of confidence in the public service' and

'Criminal offences or other conduct outside employment which would prevent an employee from continuing to do his/her job or which affects his/her suitability to perform his/her work, makes him/her liable to be unacceptable to other employees or management, or is liable to damage the Authority's business'

4.5. The way in which employees and others associated with the Council, present and conduct themselves on social networking sites can have an impact on the public perception of the Council. Everything shared on a social networking site could potentially end up in the public domain. Even where privacy settings have been set up to allow 'friends' only access, opinions expressed, information given and photos or videos posted could be seen or used by someone not originally intended.

4.6. Employees should ensure that their use of social media, either as part of their work, or in their own time, does not damage the reputation of the Council.

5. Breach of policies and/or procedures

5.1. Employees should ensure that their use of social media does not breach any of the Council's policies and procedures, or result in the Council being subject to legal challenge.

5.2. The Officer Code of Conduct, Members' Code of Conduct, ICT Policy and Disciplinary Rules are particularly relevant to the use of social media. Relevant sections of these are referred to in the following sections.

5.3. Employees should ensure that they are familiar the above documents in their entirety and with any other policies and procedures relevant to their service area.

6. Use of social media - general

6.1. There are many different types of social media. A guide to some of the most popular can be found in appendix one.

6.2. The Council recognises that social media sites can be a useful way of promoting the Council's activities and of developing and maintaining social networks. Where social media is used as part of an employee's work, he/she should ensure it is used in accordance with service policies, procedures and guidance, and the Council's ICT policy,

6.3. The Council also recognises that many employees use social media to interact socially with colleagues and friends. It is not the Council's intention to suggest that employees should not use social media in their own time. However it expects certain standards of conduct to be observed to protect its credibility, reputation and to protect employees and service users from the dangers of inappropriate use.

6.4. Front line staff (e.g. social workers, planners and environmental health officers) may wish to consider carefully how publicly their profile information can be seen, and what information to include, when setting up a social media account. Including information about their employer or type of work may enable service users to identify them.

7. Accessing social media sites whilst at work (including working at home)[1]:

7.1. Employees should not use the internet to access or update their own personal social networking sites (e.g. Facebook) or to access any other recreational sites during core working hours, as doing so means that they are wasting time for which they are being paid by the Council. Access to corporately provided Facebook pages e.g. Youth Services are exempt from this restriction.

7.2. Employees may use the Internet to access non-work related sites for personal reasons during their lunch break or before or after they have completed their working hours for the day. They should check before doing so that this is operationally convenient in their work area. They should always 'clock out' of the flexitime recording system (or the system that is in use in the work area) before using the Internet for non-work purposes.

7.3. These rules apply whether the internet is being accessed via the Council's ICT equipment, or employees' own devices e.g. smart phones.

7.4. It is important that access to the internet in WBC is used responsibly and legally. Users must not take any action which could bring the Council into disrepute, cause offence, interfere with the individual's or organisation's work or jeopardise the security of the Council's ICT systems, software or data.

[1] These rules about accessing social media sites using the internet can be found in the Council's ICT policy.

8. Using social media outside work

8.1. Employees and others associated with the Council should be mindful that anything posted on social media sites, even where privacy settings have been used, could become publicly available. When posting comments, opinions photos and/or videos on social media sites they should take care that they do not do anything that breaches confidentiality, which could bring the Council into disrepute or which breaches Council policies. They should consider whether they would say or display what they are posting publicly, to an unknown audience.

8.2. It is recommended that Council employees do not identify that they work for the Council on social networking sites as this could directly link their behaviour outside work to the reputation of the Council.

8.3. Business networking sites (e.g. LinkedIn) require the user to give information about their employer and job role, and this profile information and comments posted can be seen by a wider range of people than those directly known by the user. Extra care should be taken when posting comments on these sites

8.4. The Council recognises that there are times when employees may feel the need to 'let off steam' about work. However doing so on a social networking site could damage the reputation of the Council and could be in breach of Council policies. Employees should use official ways of discussing work issues such as one-to-one or supervision meetings, appraisals and, where appropriate, the Grievance Procedure or Confidential Reporting Code (Whistle blowing Policy).

8.5. It is recommended that Council employees should not be 'friends' with service users who are vulnerable adults or children, as this could be regarded as a safeguarding issue

8.6. Unauthorised use or disclosure of confidential information gained through employment (or other association) with the Council or failure to protect such information will be treated as misconduct, unless the disclosure is protected by law.[2]

9. Examples of unacceptable use of private social media

9.1. The following list provides examples of behaviour which the Council would consider unacceptable and could lead to disciplinary action being taken against an employee. Please note this list is **not** exhaustive:

- Posting things that bring the Council into disrepute or could result in legal challenge to the Council
- Posting things that would breach council policy, the Code of Conduct, or disciplinary rules
- Using the Council's logo or giving the impression that you are expressing the views of the Council
- Posting personal details e.g. addresses and/or phone numbers, or photographs of service users or commenting about service users.
- Posting contact details or photographs of colleagues without their permission.

[2] See the Code of Conduct for Officers (section 7) and Code of Conduct for Members (section 4)

- Divulging confidential information about, or belonging to the Council.
- Make offensive or discriminatory comments or posts about the Council, service users or colleagues. This may amount to cyber-bullying, harassment or defamation.
- Setting up or accepting vulnerable adults or children who are service users, as friends or associates.

9.2. If an employee is unsure whether it is acceptable to post something on a social media site he/she should check with his/her line manager before doing so.

Appendix One – examples of popular web and social networking sites:

Facebook - a social networking service where users create personal profiles, add other users as friends and exchange messages, including automatic notifications when they update their profile. Additionally, users may join common-interest user groups, organised by common characteristics (e.g. workplace)

Twitter - a microblogging service* enabling its users to send and read publicly visible messages called 'tweets'. Tweets are text based posts of up to 140 characters displayed on the user's profile page. Users may subscribe to other users' tweets.

LinkedIn - a business related social networking site mainly used for professional networking. Users maintain a list of contact details of people with whom they have some level of relationship, called 'connections'. This list of connections can then be used to build up a contact network, follow different companies and find jobs, people and business opportunities.

MySpace - an online community of users' personal profiles. These typically include photographs, information about personal interests and blogs*. Users send one another messages and socialise within the Myspace 'community'.

YouTube - a video-sharing website on which users can upload, share and view videos. A wide variety of user-generated video content is displayed, including film and TV clips as well as amateur content such as video blogging*. Media corporations including the BBC also offer some of their material via the site. Most videos enable users to leave and exchange comments.

Wikipedia - a collaborative web-based encyclopaedia project; its 18 million articles have been written collaboratively by volunteers around the world, and almost all articles are freely editable by any visitor. A prominent web 2.0 site but not an example of a social networking site per se.

*A 'blog' is a type of website usually maintained by an individual with regular entries of commentary and descriptions of events (blogging). The contact of a microblog is simply smaller in size.

Source: 'Social Networking' – a report by the Institute of Employment Studies.

Photo sharing websites - e.g. Flickr