East Herts Council

Social Media Policy

Policy Statement

Policy Statement No 43 (Issue No 1)
October 2012

Contents

SOCIAL MEDIA POLICY
Policy Statement No 43 (Issue No 1) October 2012

1.0 Background

1.1 Social media opens up many new and exciting opportunities. The Council's Social Media Principles (Appendix A) will ensure these are maximised for the Council. However, there are many potential issues to consider – as individuals outside work, as employees and as an organisation.

1.2 This policy provides clear guidance about personal and business (on behalf of the Council) use of social media. This policy is part of the Information Security Policy and links with the Council's other ICT User Policies and the Officer Code of Conduct, in particular the Disclosure of Information.

1.3 Employees who fail to follow these guidelines may be subject to disciplinary action in accordance with the Council's Disciplinary Policy.

2.0 Personal Use

2.1 Using Council ICT

2.1.1 The Council allows limited personal use of ICT resources, including the internet. Please see the ICT User Policies for further information. Employees accessing social media sites on their personal devices should only do so in their own time e.g. lunch time.

2.1.2 Employees are not allowed to use Council ICT equipment to use social networking sites inappropriately or create new internet sites that contain Council information without authorisation from the Communications Team.

2.1.3 The Council reserves the right to monitor employees internet usage and where possible will endeavor to inform an employee when this is about to happen and the reasons for it. The Council considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- Been spending an excessive amount of time viewing websites that are not work-related;

- Using the internet for cyber bullying; or
- Acted in a way that could damage the reputation of the Council or breaches confidentiality
- Accessing websites deemed inappropriate as detailed in the ICT Internet Use Policy.

2.1.4 If appropriate, disciplinary action may be taken in line with the Council's Disciplinary Policy.

2.2 Personal Posting on Social Media

2.2.1 Many Council employees will have their own social networks to keep in touch with friends and family. The Council respects the employee's rights to a private life.

2.2.2 However East Herts Council must ensure confidentiality and its reputation are protected along with ensuring that customers are safeguarded. Employees should be aware that social networking websites are a public forum and should always assume that their entries on any website are public and can be seen by everyone, this could include a colleague, your manager, a Councillor and our customers.

2.2.3 The Council therefore requires employees using social networking sites to consider the Officers' Code of Conduct and not:

- Comment on the work of the Council such that it could bring the authority into disrepute.
- Comment on other members of staff or Members of the Council.
- Conduct yourself in a way that could bring the authority into disrepute.
- Allow your interactions to damage working relationships between members of staff, Councillors and any of the Councils' residents, clients or customers.

2.2.4 As an extra precaution employees may also want to consider refraining from identifying themselves as working for the Council on their own and other people's social media sites. However, if employees are commenting on a post, or posting something themselves, that is related to the Council, or a Council project, they should make it clear that they are an employee of the council.

2.2.5 The Council will not actively monitor the personal, social media profiles of staff; however if the Council becomes aware of any activity breaching the above, any investigation may include a review of activities on social media.

3.0 Business Use (On Behalf of the Council)

3.1 Setting up New Social Media

3.1.1 Employees who wish to set-up new social media profiles, pages or networking sites on work related projects or issues, must seek authorisation from the Communications Team. The Council must have an oversight of all social media channels the Council is using. The Council must also ensure that there are adequate levels of governance over social media.

3.2 Posting on Social Media for Work Use

3.2.1 The Officer Code of Conduct sets out the standards of conduct required of Council employees. These standards apply equally to conversations undertaken through the use of online media as they do to face-to-face conversations. Employees should familiarise themselves with the requirements of the Officer Code of Conduct.

3.2.2 Social media is used by a number of customer groups. When working with children employees must ensure that they establish safe and responsible online behaviours. This means working to the Council's Safe Guarding Children Policy.

3.2.3 Only employees who have been trained in using social media are permitted to post content to the Councils own social media channels or post content to other people's social networks on behalf of the Council. If employees want to join a conversation they must do this through the Communications Team.

3.3 Social Media Connections

3.3.1 The Council may choose to 'follow', 'like' or otherwise establish connections with other organisations and individuals using social media. This enables the Council to maintain contact with what other social media users are saying and, where appropriate, share their content. Sometimes we also need to establish a connection so that we can engage with users, e.g. via direct messages or posting.

3.3.2 There is no fixed approach on who the Council will have in its network, but as a guide, the audiences identified in the Communication Strategy will be considered as potential connections. Some general guidelines for staff establishing connections are:

- Be aware of connecting with commercial profiles/site; if there is a pre-existing partnership such connections can be beneficial, but employees should avoid giving the impression of endorsement or bias.
- Be aware of connecting to political or politically motivated groups.
- Should a connected organisation or body make public statements (through either social media or any other channel) that are directly contradictory to the council ethos or priorities, employees should carefully consider if they wish to remain connected.
- Should a connected profile/page/site become a platform for conflict or abusive argument, employees should carefully consider if they wish to remain connected.

3.4 Social Media and Recruitment

3.4.1 Unless it is in relation to finding candidates, (for example, if an individual has put their details on social media websites for the purpose of attracting prospective employers), Managers should only conduct searches, either themselves or through a third party, on social media when these are directly relevant to the applicants skills or claims that they have made in the recruitment process.

For example:

- A prospective employee may claim that they have used social media in their previous job (for example as a publicity tool); or
- A prospective employee's social media use may be directly relevant to a claim made in their application (for example, if they run a blog based around a skill in which they claim to be proficient).

3.4.2 Social networking sites may be used by Human Resources to advertise vacancies in appropriate circumstances.

4.0 <u>Legal Considerations and Compliance</u>

4.1 Legal Framework

4.1.1 Any form of communication has the possibility of being misunderstood and social media is no more or no less vulnerable. The following laws apply with online participation of any kind:

- Data Protection Act 1998
- Defamation Act 1996
- Human rights Act 1998
- Equality Act 2010
- Copyright, Designs and Patents Act 1988
- Regulatory and investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

4.2 Data Protection

4.2.1 People post information on social media about all sorts of things, including, for instance, political opinions. In many cases, their username, their biographical details or their link to their website makes their offline identity traceable.

4.2.2 The DPA allows employees to process personal data as an individual if it is for purely domestic purposes. This is to allow employees to keep an address book or similar. If employees are engaging in social networking for work purposes, or for research, careful consideration of the DPA is required. The Council's Information Manager must be notified of Social Media in use and its purpose, in case the use must be included within the Council's notification to the Information Commissioner.

For example:

- Referring to someone as, for instance, @JoeBloggs identifies him or her as an individual. Mentioning someone in a Tweet means employees are transferring personally identifiable information out of the European Union if the social media site is hosted outside it,
- Using a Twitter client, which will keep a subset of people employees follow on their computer, may contravene the DPA, especially if their tweets (or others' tweets about them) mention sensitive information and if they have set their Tweets to be protected.
- Creating a 'mashup' of Tweets to demonstrate a point may be an issue.

As a result:

- Do not publish the personal data of individuals.
- Do not re-publish the personal data of individuals even when they have chosen to publish it.
- See advice before analysing or using any posts on social media as this may be regarded and need consideration under the processing of personal data.

See the Council's Data Protection Policy and Information Security Policy for further guidance.

4.3 Libel

4.3.1 Employees should not publish an untrue statement about a person that is damaging to their reputation or allow someone else to publish something libellous on the Council's website or social media platforms – if employees see such a statement they must take prompt action to remove it by contacting the Communications Team.

4.4 Copyright

4.4.1 Placing images or text on any East Herts website from a copyrighted source (for example extracts from publications or photos) breaches copyright. Employees should avoid publishing anything they are unsure about, or seek permission in advance.

4.5 Bias and Pre-determination

4.5.1 Employees should avoid publishing anything that might suggest they do not have an open mind about a matter/decision they may be involved in determining. For example if employees are involved in determining planning or licensing applications or other decisions, the decision runs the risk of being invalidated.

4.6 Obscene material

4.6.1 Publishing anything that people would consider obscene is a criminal offence.

5.0 Policy Review and Amendment

5.1 This Policy will be reviewed within two years or sooner in line with legislation and best practice to reflect the best possible level of support and management.

Social Media Principles

It is part of East Herts Council's Communication Strategy to engage effectively with social media. We have both an opportunity and a responsibility to manage and protect the council's reputation online and to selectively participate and engage in the online conversations that mention us on a daily basis.

Our Communication Strategy encourages officers and councillors to participate appropriately in social media and has created an official presence on many social media platforms. These principles exist to empower officers and councillors to participate in online communities.

Eight Expectations for PROFESSIONAL online activities
Speaking 'on behalf of' East Herts Council

- **Attend training:** All employees who wish to represent East Herts Council online must complete the Social Media Certification Training prior to doing so.
- **Follow our performance, conduct and behaviour policies:** The Officers' Code of Conduct sets out the standards that all employees should maintain in the workplace, and this includes online work. Be respectful, how you act online affects the reputation of you, your colleagues and the Council.
- **Identify yourself as a representative of East Herts Council:** at the outset, you must state your name and the service you are representing. It is never acceptable to use aliases.
- **Monitor your relevant social media channels:** Make sure that you know what is under discussion, so you can respond when needed.
- **Keep records:** Online conversations are often short-lived and instant and therefore it is vital that that we keep records of our interactions. Remember that online statements could be to the same legal standards as traditional media communications.
- **If in doubt, do not post.** Online spokespeople must ensure that posts are accurate and do not contain non-public information concerning East Herts. When in doubt, do not post; instead contact the Communications Team for further guidance.
- **Respect copyrights:** Always gain approval from, and give credit to, the owners of any content you publish online. For example; images, video, text, music and trademarks
- **Protect data:**

Four Expectations for PERSONAL online activities

Speaking 'about' East Herts Council

- **Keep an eye out for compliments and criticism:** You are a vital asset for monitoring social media platforms. If you come across positive/ negative comments online about East Herts Council, that you consider important, then forward them to the Communications Team.
- **You are responsible for your actions:** When conversing online follow the Officer's Code of Conduct. Any action online, which could potentially damage the reputation of East Herts Council, will ultimately be your responsibility. Do not disclose information that is not publicly available. Engage, but use common sense.
- **Be conscious about mixing your personal and business lives:** Online, personal and business lives cross paths. Internal and external corporate contacts, as well as the East Herts community may have access to what you post, even if this was not your intention. Speaking about them in a negative, demeaning or offensive way is not acceptable.
- **Remember data protection guidelines!!!**

Reputation Management

There are particular rules of engagement to consider for crisis response situations. For example, deleting a post or blocking a user may escalate the issue, rather than resolve it. If you become aware of a comment, post or content that is inappropriate or poses a risk to East Herts Council's reputation please bring it to the attention of the Communications Team.

Social media is continuously evolving and therefore these principles will be updated alongside the annual review of the Communication Strategy.