APPENDIX H

Sheffield City Council

Social Networking Policy

Publication Date: July 2015

Author: HR Service

Document Control

Organisation	Sheffield City Council
Title	Social Networking Policy
Owner	HR Service
Subject	Conduct and Work Relationships
EIA required	Completed 13/07
Review date	01/04/2016

Revision History

Version	Revision Date	Reviser	Previous Version	Description of Revision
1.1	15/05	LP	1	Minor amendments - Updated hyperlinks for new Information Governance and Security Policies

Document Distribution – Approval and Release

Decision Maker	Approval date
Full Council	15/07

Social Networking Policy

1. Purpose

It is very much in our (the Council's) interest to allow you (the employee) to participate in this rapidly growing environment of relationships, learning and collaboration.

This policy provides you with a set of principles for using social networking sites responsibly, which is linked to the Officers' Code of Conduct and associated policies. It gives you clear guidelines, so you can protect yourselves by complying with our conduct rules, with the laws on harassment, discrimination, data protection, copyright and ensuring your own safety.

The policy ensures that we are not exposed to financial, legal and governance risks and that the safeguarding of children, young people and vulnerable adults is not threatened by the use of social networking

As this is a new policy, which is to be used across the organisation and everybody is impacted by it, it is important that this is reviewed regularly, initially by Executive Management Team after 6 months.

2.0 Introduction

Sheffield City Council recognises that the internet provides unique opportunities to participate in interactive discussions and share information using a wide variety of social networking sites.

We believe in open exchange using social networking sites to empower you and customers. These individual interactions represent a new model: not mass communication but masses of communicators. Through these interactions, you and

local people are empowered to learn, share your expertise and promote what is best in Sheffield.

- You can contribute best practice on our services - sharing your expertise, raising Sheffield's profile.

- Through individual interactions, you can better involve and engage with a wider range of people, including young people and people setting up new businesses in the city. This allows us to learn from our customers, drawing on their expertise and knowledge to design services that meet their needs.

- By encouraging local people to contact us using social networking sites – e.g. via e-petitions - we can gain information on key issues to help inform policy in the city.

- Use social networking as a technology platform for open innovation and learning, which makes it easier for you to learn, develop, reflect on practice, be creative and collaborate for improved services.

Whilst we have embraced these technological innovations as part of our working and private lives, employers are now grappling with consequences of unacceptable posts, which are rapid communicated and shared. We have recently dealt with social networking issues relating to:-

- Bullying and harassment,
- Freedom of expression of political views
- private/professional boundaries with children
- problems with blurring private/professional boundaries – manager/employee
- work-related offensive photos
- being off sick and using social networking for secondary employment
- Employee petition against service closures.

In many of these cases, the employees were unaware that social networking is not private and that there are potential consequences to their on-line activity.

Managers, Trade Union Representatives and HR Practitioners have therefore asked for helpful, practical advice to protect you and us, when you use social networking sites in a work and private capacity. Representatives from all these groups, plus Members of the Equality Forums have contributed to this policy.

3.0 Scope

This policy applies to all non-schools based Sheffield City Council employees, casual workers, agency staff, contractors, consultants, self-employed people, apprentices, trainees and those on work placements, who work for the Council. Throughout this policy, the term 'employee' and 'you' is used to cover all these types of workers. The Social Media Policy adopted by the relevant Governing Body will apply to teaching and support staff in schools.

This policy deals with the use of all forms of social networking including but not limited to Twitter, MySpace, Facebook, texts, emails, BlackBerry Messenger (BBM), LinkedIn, Blogs, Wikipedia sites and any other sites which involve document, photo or video sharing such as YouTube or new networks, internet sites/channels that may be developed in the future.

This policy applies to the use of social networking for both work and personal purposes, whether during working hours or otherwise and whether at work or elsewhere including in your home. It also applies regardless of whether the social networking site is accessed using our ICT facilities/equipment or that belonging to you.

This policy should be read in conjunction with:
- Officers' Code of Conduct and associated policies
    - Member-Officer Relations Protocol
    - Information Governance and Security Policy
    - ICT Acceptable Use Policy
    - Data Protection Policy
    - Dignity and Respect at Work Policy
- Social Networking Guidance
- Draft Safeguarding Children and Vulnerable Adults Policy
- Disciplinary Procedure
- Recruitment and Selection Policy
- Social Media Position Statement, EMT (June 2011)

Responsibilities

The Council

We recognise the benefits of social networking and trust you to act responsibly. We expect you to work in the same way on-line and off-line, following the behaviours set out in the Officer Code of Conduct, as detailed in this policy and in associated guidance.

We permit personal use of social networking sites at work during break times as long as it is not excessive and/or does not involve unprofessional or inappropriate conduct and does not interfere with your responsibilities or performance. You need to bear in mind that you must take short breaks away from screens to protect your health.

We also know that some employees and their managers need to consider safety of their service users and themselves, if they use social networking sites. These sites are public and there is a possibility that employees or service users could be traced, resulting in harm to that person. Where this is an issue, employees and their manager will need to carry out a risk assessment for using social networking for work purposes.

Employees

You are personally responsible for the content you publish on-line and must be mindful that **everything placed on-line is public** and is hard to remove once posted.

You should follow our social networking principles, which are divided into 4 themes, with the core behaviours applying across the themes.
In brief, you should:-

- Be professional when using social networking for work and personal use
- Be respectful at all times, never post offensive or intimidating texts or images about a person
- Familiarise yourself with this social networking policy and associated guidance

You are responsible for the success of this policy and should ensure that you take the time to read and understand it. You should report any misuse of social networking to the appropriate line manager.

Managers

All managers have a specific responsibility for operating within the boundaries of this policy. You must ensure that your employees understand the standards of behaviour expected of them and take action if behaviour falls below the required standard.

Managers should:
- Familiarise themselves with the Social Networking Policy and guidelines
- Ensure their staff are aware of the policy
- Take prompt action to stop any harassment or bullying they become aware of, whether a complaint has been raised or not
- Support the staff involved in any allegations about cyber bullying, harassment, discrimination, using existing procedures
- Ensure all complaints/allegations are dealt with fairly and consistently and in line with other employment policies.

HR and Trade Unions should

Provide support and advice to managers and employees on the operation of the policy and guidelines, where necessary.

Compliance

You must comply with Council policies and the law when using social networking sites. Make sure that you:-

- Know and comply with the Officers' Code of Conduct and associated policies including the Dignity and Respect Policy, Information Security Policy and E-Communications Guidance.

- Only share public information on-line. Information that is not public, such as service user, employee or manager information given in confidence, may only be shared in accordance with the law. If you use non-public information inappropriately, you may be personally prosecuted under the Data Protection Act.

- Are professional, when posting comments about the Council and our services. Be aware that the Council may take disciplinary action, if there is a reasonable belief that your on-line comments have damaged the Council's reputation.

- Are respectful at all times to our customers and colleagues. Never post offensive or intimidating texts or images about a person.

You are expected to use the **same professional behaviours on-line,** as you would when communicating with service users and colleagues **off-line.** You must not post any information or messages on-line, that you would be unwilling to say in public face to face. Make sure that you follow the principles and standards set out in this policy, in the Officer Code of Conduct and associated listed policies.

Where your manager identifies that you may have fallen short of the standards in this policy, your manager is to deal with the matter informally where appropriate. The formal procedure will be used however, to guide you towards achieving acceptable standards as set out in this policy.

You may have disciplinary action taken against you, if you do not keep to this policy, which includes the possibility of being dismissed without notice being given. Serious breaches of this policy for example incidents of bullying on social networking sites may constitute gross misconduct and 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. You are required to co-operate with investigations into allegations made under this policy.

You must not make false or malicious allegations about another person's use of social networking and need to be aware that disciplinary action may be considered in such circumstances.

You may be required to remove social networking posts, which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Social Networking Principles

Personal Use

1. Be professional, know and follow the Officer Code of Conduct. You are personally responsible for what you post. Be thoughtful about how you present

yourself in social networks. Understand that social networking is a public forum and your entries are not private and are hard to remove once posted.

2. We can ask you to remove on-line content if we have a reasonable belief that it is damaging the Council's reputation. If we can prove that your conduct on-line has caused detriment, you may face disciplinary action and if severe enough, you could be dismissed as a result.

3. You have a right to express political and religious views, as long as they are lawful, are made in a private capacity and do not impact on your job. Some employees are in politically restricted posts and need to maintain political impartiality.

4. Do raise any work-related concerns in the right way. You can speak to your manager, give feedback in the employee survey, attend staff forums, speak to a contact advisor, contact your trade union representative, get support from the independent employee assistance programme or for serious allegations, use the whistle-blowing procedure. This allows us to investigate and address the issue in the first instance.

5. As you are an employee of the Council, you must ensure that your on-line content is consistent with your professional image that you present for the Council.

6. Be respectful of other employees, service users or customers as set out in our [Dignity and Respect at Work Policy](#).

7. There is no expectation for you to accept 'friend' requests from colleagues or managers

8. You are allowed appropriate and reasonable personal use of social networking at work, using Council or your own equipment. This is to take place in your own time and outside core hours, not adversely affecting performance or provision of service. Personal use of Council equipment is at no additional cost to the Council.

Business Use

9. When acting on behalf of the organisation, you must be professional. Always be responsible for your on-line comments, be credible, accurate and fair. Make sure that you are respectful at all times, especially when replying to disagreements. Avoid unnecessary or unproductive arguments. Do not speculate about an issue or start inflammatory debates. Make sure what you say is factually correct.

10. If you have any doubts about content, do not post without escalating to a manager. If you make an error, be up front about your mistake and correct it quickly, as this can help to restore trust. If your mistake is serious, let your manager know immediately and get advice. Ultimately, you are responsible for what you post or publish on a social networking site.

Maintaining Professional Relationships

11. You have a specific duty of care to take reasonable steps to protect service users, colleagues and yourself from harm. You must discuss any safety issues of using social networking sites for work purposes with your manager and if relevant draw up a risk assessment. This may state that you must only use secure forms of communications for work purposes. If you receive a serious on-line threat to life or buildings, you must contact the police immediately and let your manager know.

12. If you are in a **position of trust** with **Children** or **Vulnerable Adults**, for example if you work in social care, you have a professional relationship with your service users. You must draw a line between your professional and private life.

    You must not strike up or accept an on-line relationship with your service users, using a personal social networking account. This applies even if your service users are no longer receiving a service.

    Similar to your off-line work, where you have a close relationship with a service user, you must let your manager know.

    In these circumstances, you must declare any interest you may have with a person, which may cause a direct or indirect conflict of interest with your employment. This information is provided to protect you and service users against any allegation of favour or disadvantage.

13. If you interact with **Elected Members** on social networking sites, you must follow the existing rules within Officers' Code of Conduct and Member-Officer Relations Protocol. Officers in politically restricted posts must be particularly carefully to be impartial and maintain professional relationships.

Gathering and Sending Out Information

14. You can provide any Council Public Information to social networking sites. This is information, which is already in the public domain. You must keep non-public information secure and never release this to social networking sites. Non-Public Information includes personal data about service users or employees. If you suspect that any of your social networking accounts have been hacked, resulting in an impact on your work, you must let your manager know immediately.

15. Any monitoring or surveillance of a customer or employee is strictly controlled and you must be authorised to carry out this activity. For example, you must never become a 'friend' of any service user or employee for the purpose of obtaining information, unless authorised.

16. We reserve the right to monitor your social networking and internet use at work. Valid reasons for checking your usage include suspicions that you have:

- Been spending an excessive amount of time viewing sites that are not work-related or
- Acted in a way that damages the reputation of the Council and/or breaches disclosure of non-public information