St.Helens Council

# Social Media Policy

**Version:** 3.0

**Date:** May 2018

# Version Control

| Date | Version | Comments |
|---|---|---|
| December 2011 | 1.0 | First finalised version |
| September 2015 | 1.1 | Policy subject to a full review |
| December 2015 | 1.2 | Draft approved at IMG |
| February 2016 | 1.2 | Union Consultation |
| March 2016 | 2.0 | Approved by Executive Decision |
| April 2017 | 2.1 | Annual review |
| May 2018 | 3.0 | Review for legislative changes (GDPR) |
| | | |

# Table of Contents

# 1 Introduction

1.1 The Council will use Social Media tools to engage with the public where it is considered that such tools will provide an effective means of community engagement. However, safeguarding the reputation of the Council will remain the key consideration in determining how and when Social Media is used.

# 2 Policy Statement

2.1 The purpose of this Policy is to assist employees by providing clear guidance about acceptable behaviour on Social Media both in and out of work. It is consistent with the Regulations and Conditions of Service which employees should already be aware of in their work for the Council.

2.2 The Policy seeks to ensure that the reputation of the Council is not adversely affected through our use of Social Media, and that the Council is not exposed to legal and governance risks that can be very significant.

# 3 What is Social Media

3.1 Social Media is defined as 'websites and applications that enable users to create and share content or to participate in Social Networking'.

3.2 Social Media tools include, but are not limited to:

- Blogs/Microblogging e.g. Twitter
- Social Networking e.g. Facebook, Foursquare
- Collaboration networking media
- Social bookmarking
- Photo and video sharing e.g. Youtube, Flickr, Snapchat
- RSS aggregation services
- Wikis e.g. Wikipedia

3.3 Social Networking is defined as 'the use of dedicated websites and applications to interact with other users or to find people with similar interests to one's own'.

# 4 Scope

4.1 This Policy applies to all Employees. For the purpose of this Policy the term 'Employee' refers to all full-time and part-time employees, temporary employees, agency workers, contractors and consultants.

4.2 This Policy applies to the use of Social Media for both business and personal purposes, either during working hours or outside of work. It also applies whether the Social Media is accessed inside or outside of work and either using Council or personal IT facilities.

4.3 This Policy should be read in conjunction with the Code of Conduct for Employees, the Council Comprehensive Equality Policy and other associated relevant policies, procedures and guidance as contained within the Information Management Framework and document library.

# 5 Key Principles

5.1 You must be conscious at all times of the need to keep your personal and professional lives separate. You must not put yourself in a position where there is a conflict between your work for the Council and your personal interests.

5.2 The Council needs to ensure that its reputation is not damaged and confidentiality is not breached by:

- Revealing information owned by the Council.
- Revealing or sharing confidential information about an individual (such as a colleague or service user).
- Discussing the Council's internal workings (such as spending or business plans that have not yet been communicated to the public).
- Sharing confidential or sensitive information about individuals gained through your employment.

5.3 The public and our partners must be able to trust the integrity of our employees. Therefore you must not engage in activities involving Social Media which might bring the Council into disrepute e.g. criticising the Council, service users or colleagues in an inappropriate manner, posting images that are inappropriate or links to inappropriate content. Furthermore, the Council may be liable for the actions of staff who post inappropriate content on social media.

5.4 You must not represent your personal views as those of the Council.

5.5 Any information published online can be accessed around the world within seconds and will be publicly available for all to see, this can be regardless of privacy settings, and is not easy to delete / withdraw once published. The Council views all comments made on Social Media sites are done so publicly, and that any inappropriate comments made will be considered in the context in which they are made.

5.6 The Council logo, or other devices must never be used on Social Media tools that are unrelated to, or are not representative of, the Council's official position or which do not conform to the conditions within this Policy.

5.7 Where your post is classified as 'politically restricted' (as defined in the Code of Conduct for Employees) you must not write or speak publicly (other than in an official capacity) with the intention of affecting public support for a political party.

# 6 Social Media for Business Use

6.1 A Business Case must be completed by the appropriate Service Manager, and agreed by the Service Delivery - Customer Services Section in the Corporate Services Department.

6.2 Social Media accounts may only be created by members of the Service Delivery - Customer Services Section.

6.3 A Social Media User Agreement must be signed by the appropriate Employee who must ensure it is abided by at all times.

6.4 Social Media must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the Council into disrepute.

6.5 Council representatives should identify themselves as such where appropriate on Social Media tools. This would include providing additional and appropriate information in user profiles.

6.6 Council representatives should ensure that any contributions they make are professional and uphold the reputation of the Council and are in accordance with the conditions of this Policy.

6.7 Any Social Media website or link that is being officially used by the Council should be explicitly referred to on a section of the corporate (www.sthelens.gov.uk) website homepage or Social Media page, so that users of online services can determine if content on a site or link is being legitimately provided by the Council.

6.8 Council email accounts may be used for username logins only and must never be displayed on any website or otherwise made public.

6.9 Representatives of the Council must abide by the conditions of use imposed by any provider of Social Media they wish to use.

6.10 The use of the Council's logo and other branding elements should be used where appropriate to indicate the Council's support.

6.11 If a Council representative cannot participate in a particular Social Media while complying with its conditions of use, and within the rules imposed by this Policy, then that particular Social Media provider will be deemed inappropriate.

6.12 Each Service area should produce an appropriate procedure governing their use of Social Media which is aligned to this Policy.

6.13 Each Service area will be responsible for regularly reviewing their account and must remove any inappropriate content posted on or linked to it.

6.14 Where employees are managing Social Media tools, appropriate feedback and complaints information must be published in a prominent place, which is easily accessible to other users.

6.15 Council representatives must consult the Council's Internal Audit section wherever they feel that Social Media activity may have implications with regard to data protection legislation.

6.16 Service requests, complaints and comments made by users via Social Media tools should be referred to the Council's Contact Centre.

6.17 Communication regarding these enquiries must not be dealt with through Social Media. Only direct communication methods, such as e-mail and telephone can be used, in accordance with our professional standards.

6.18 Requests for statements from the Council or press enquiries through Social Media should be referred directly the Press Office, and managed accordingly.

6.19 Employees must not use personal devices to access the Council's Social Media Profiles.

6.20 Representatives of the Council must bear in mind that the information they share through social media, including through private spaces, remains subject to legal requirements governing publication and disclosure, including the Safeguarding of Vulnerable Groups Act (2006).

6.21 The Council's Caldicott responsibilities apply to any material that is shared through social media, and the Council's Caldicott Guardian must be made aware of any breaches of these standards.

# 7 Social Media for Personal Use

7.1 The Council respects all employees' right to a private life, however as a Council employee, you are expected to behave appropriately and in accordance with the Council's Employee Code of Conduct.

7.2 The rules governing staff conduct such as the Code of Conduct and Equality Policy still apply to your conduct outside of work. Comments and views expressed in your own time (regardless of privacy settings), which are incompatible with the Council's policies, may

lead to a loss of trust in you as an employee and could have a serious impact on your employment with the Council.

7.3 Employees are responsible for any content linked to their Social Media accounts and must ensure that any online activities/comments made on these accounts are compatible with their position within the Council, and safeguard themselves in a professional capacity. This includes all contact/content linked to their accounts including posts, re-posts, tags, comments, 'Likes/Dislikes', friend requests, 'Follows', etc.

7.4 Employees must ensure their personal Social Media accounts comply with this Policy and do not bring the Council into disrepute, this includes (but is not limited to) comments about customers, suppliers, colleagues, the Council, etc.

7.5 Employees should be aware that any offensive comments, posting inappropriate material, cyber bullying/harassment or views/associations which are inconsistent with the Council's ethos or which may damage the reputation of the Council will be considered in breach of this Policy individual e.g. making offensive or derogatory comments relating to sex, gender reassignment, race (including ethnicity), disability, sexual orientation, religion/belief or age.

7.6 Employees should not use their Council email address or other official contact details for setting up personal Social Media accounts or communicating through such media.

7.7 Employees must not edit open access online encyclopedias (or any other such material) in a personal capacity at work. This is because the source of the correction will be recorded as the Council's IP address and the intervention will appear as if it comes from the Council itself.

7.8 If you are concerned that another employee's behaviour online might have implications for the Council, you must report this to your Manager. You must not get involved directly e.g. commenting on, liking/disliking the post, etc.

7.9 Information which employees have access to as part of their employment, specifically personal or confidential information, must not be discussed on such media.

# 8 Investigations

8.1 The Council's regulatory sections, for example, Trading Standards and Counter Fraud, may need to use social media as an investigative tool to gather evidence during criminal investigations.

8.2 Personal information may be obtained by viewing a person's social networking profile and/or creating a covert relationship with a member of the public as part of a criminal investigation. Repeat viewing of open profiles via social media in investigations may constitute directed surveillance. Consideration should therefore be given to the need for internal authorisation and a Judicial Approval from the Magistrates Court in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA). The Council's RIPA Policy Guidelines provide further guidance regarding the RIPA process. It requires those designated officers who authorise the use of directed surveillance techniques to give proper consideration to whether their use is necessary and proportionate.

8.3 If any investigation is being considered you must consult the Council's Social Media Investigations Procedure, and seek appropriate advice.

# 9 Responsibilities

## Information Management Group (IMG)

9.1 The role of the Information Management Group (IMG) is to co-ordinate the approach to every aspect of Information Management, and not just compliance with DPA 1998.

9.2 The group is made up of Departmental Information Management Representatives who are senior managers in each Department and are responsible for a multi-disciplinary approach to the management of information throughout their Departments.

9.3 The IMG is responsible for the overarching governance and implementation of the Policy throughout the Council.

9.4 The IMG is responsible for ensuring that all Employees are fully aware of Council policy and process, and have received appropriate training.

9.5 The IMG is also responsible for the development and monitoring of the adherence to the Policy.

### Social Media Moderator

9.6 The main role for the Social Media Moderator will be to see that any comments posted comply with the guidance provided to participants and allow the Council to conduct Social Media activity in accordance with this Policy.

9.7 The Social Media Moderator will ensure that no material is published, either by ourselves or by third parties, that will contravene our responsibilities under this Policy, in particular:

- disclosure of personal information in contravention of data protection legislation;
- material of an offensive nature;
- images of a pornographic or otherwise offensive nature;
- material that is of a racial, homophobic or otherwise discriminatory nature, and that may constitute incitement;
- material of a defamatory nature;
- material that breaches our safeguarding responsibilities; and
- any other inappropriate material of the type considered in section 5 of this Policy.

### Line Managers

9.8 Line Managers are responsible for ensuring all Employees in their operational area adhere to the Policy and have undertaken all relevant training.

9.9 Line Managers are responsible for ensuring that Moderators and any Social Media accounts within their control are monitored effectively and operate within the Policy.

9.10 Line Managers have a responsibility to ensure that all potential breaches of this Policy are reported to the appropriate Departments in a timely manner.

9.11 Line Managers must complete a Social Media Business Case and have this approved by their Service Manager.

9.12 Line Managers must ensure that the Social Media User Agreement is completed and abided by.

### Employees

9.13 All those covered by the scope of this Policy are responsible for ensuring that their use of Social Media is in line with the Policy.

9.14 All those covered by the scope of this Policy must undertake all relevant training in Social Media.

## 10 Review and Governance

10.1 The Policy will be subject to governance through the Information Management Group (IMG), and will be formally approved by Chief Officers Group via the Executive Decision Framework.

10.2 The Policy will be subject to at least an annual review, and where changes in legislation require, more frequently.

# 11 Policy Compliance

11.1 If you are found to have breached this Policy, the matter will be considered and investigated under the Council's disciplinary procedure.

11.2 Serious breaches of this Policy e.g. incidents of bullying of colleagues, discriminatory behaviour or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal. Breaches, where applicable, may also result in civil action and/or criminal charges.

11.3 Social media content which proves that employees have breached other Council policies may be used in disciplinary investigations relating to these matters.