# **Sefton Council Social Media Policy**

**Section:** Conduct in the Workplace

**Source:** Cabinet Member - Corporate Services – 12<sup>th</sup> August 2013

Issue Date: 20th August 2013

Amended: October 2013, January 2014, June 2018, June 2019, June 2022,

February 2023, July 2023

Appendices: 1. Social Media Business Case Form 2. Website Unblocking

Form

#### 1. Introduction

1.1 Communications are at the core of every service delivered by Sefton Council. Good and clear communication is the responsibility of <u>everyone</u> employed by the council.

- 1.2 There will always be the need to offer choice to our residents and the ability to interact via the channels that they want to use.
- 1.3 This includes the continued use of traditional communication methods alongside social media.
- 1.4 The policy must be read in conjunction with the Internet and E-mail policies and Social Media Advice and Top Tips from the Corporate Communications Team.

#### 2. Definition

- 2.1 For the purposes of this policy, social media is any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum.
- 2.2 This includes (but is not limited to) online social forums such as Twitter, Facebook, Instagram and LinkedIn, as well as blogs and video or imagesharing websites such as YouTube and Flickr.

#### 3. Policy Statement

- 3.1 The Council acknowledges that there are significant opportunities in using social media and the responsible, corporate use of social media is continuously being developed.
- 3.2 The policy provides clear guidelines for using social media sites to ensure they are used effectively as part of a wider communications mix and that their use does not expose the Council to security risks or reputational damage.

# 4. Scope

4.1 The social media policy covers all employees who have a contract of employment with Sefton Council, or who work on behalf of Sefton Council.

- 4.2 This also includes temporary contracts, agency workers, contractors and employees on secondment from other organisations.
- 4.3 The contents of the policy cover social media use inside and outside the workplace both during work hours and outside normal working hours.
- 4.4 The policy applies regardless of whether the social media is accessed using the Council's IT facilities or equipment belonging to individuals.

# 5. Use of Social Media for Work Purposes

- 5.1 Social media websites are currently blocked for most users. However, if teams wish to use social media specifically for their area of work the Website unblocking form should be completed and submitted to the ICT helpdesk for approval by the Authority's Computer Auditor. Where applicable, an approval email may also be required from the individual's Assistant Director.
- 5.2 In circumstances where a social media account is required e.g.
  Twitter/Facebook, a Social Media Business Case should be completed. This
  will be submitted to the Corporate Communications department, who consider
  the evidence and have the final say on the approval of accounts.
- 5.3 Any communications that employees make through social media *must not:* 
  - a) Be offensive, discriminatory, defamatory or make inappropriate comments about the Council, it's customers, service users, suppliers or any of its employees
  - b) Be in breach of Data Protection regulations by using images, video and audio files without consent (see 5.5).
  - c) Divulge confidential or personal information about, or belonging to the Council, its service users, customers or suppliers
  - d) Publish anything which may have the potential to bring the Council into disrepute
- 5.4 Access to social media and networking sites is provided for work purposes only. Such websites should not be accessed for personal use at any time e.g. during work hours or lunch breaks.
- 5.5. Consent must be obtained in writing and set out in a particular way, **depending** on the circumstances of the case. If any employees are unclear as to when consent is appropriate, you must take advice from Corporate Legal Services. (A photo consent form is available on the intranet to record the consent in writing).
- 5.5.1 Taking photographs/ videos of employees and posting on social media
- 5.5.1.1 If you take a photograph of a member of staff intending to post on social media, you must obtain valid consent. This means that the employee must agree in writing to their photo to be published on a particular social media site and also must feel that they can decline and not be put under any undue pressure to having the photograph or image and sign the consent form.

- 5.5.1.2 Example: If the Council takes a photograph of a member of staff winning an award, we should still get their consent to posting that photograph on social media. If the award organisers (i.e. a different organisation) takes the photograph it is incumbent on that organisation to get consent or the member of staff to refuse the photo.
- 5.5.1.3 The ICO states: 'Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident, they can demonstrate it is freely given'. Also, "Consent will not usually be appropriate if there is a clear imbalance of power between you and the individual. This is because those who depend on your services, or fear adverse consequences, might feel they have no choice but to agree so consent is not considered freely given. This will be a particular issue for public authorities and employers'

# 5.5.2 Taking photographs of the public and posting on social media

- 5.5.2.1 Service areas often wish to celebrate and publicise events during the course of providing services to the public and may wish to post images of events on social media sites. All images of the public (where the member of the public can be easily recognised) posted on social media using the Council's social media pages must obtain valid, written consent of the persons involved using the appropriate consent form.
- 5.5.2.2 Employees, in their professional capacity, must never use their own personal media sites to post images of members of the public or employees, unless they have the permission of the corporate Communications team and have first taken advice from Corporate Legal Services. However, employees can re-post official Council social media posts.
- 5.5.2.3 To be clear, if a member of staff takes a photograph at the Southport Flower Show (for example), in their private capacity, such images are not covered by this policy.

#### 5.5.3 Protocol for social work staff

- 5.5.3.1 Workers should also be sensitive to what photography might mean for a child/young person now and in the future.
- 5.5.3.2 It is recognised that taking photos or videos of children/young people is a legitimate, and indeed an essential part of working with them, such as the recording of activities, at the request of the child or young person themselves, or for life story work. In all such situations staff should alert their line manager to the fact that photos or videos are being used and this should be recorded clearly in supervision notes.
- 5.5.4 <u>Protocol to be followed by social work staff when photographing or taking videos of children/young people</u>
- 5.5.4.1 The use of photography or reproduction of photographic images or the use of videos must always have a clear and child-centred purpose.
- 5.5.4.2 Prior to the taking of any photo or video the purpose of this should be explained to the child or young person according to their age, development and understanding and to the parent/carer unless there are specific reasons

- not to do so in which case the child's/young person's social worker must give permission. A child or young person should not be photographed if they do not wish to be or if their parent/carer/worker does not wish them to be.
- 5.5.4.3 In relation to one-to-one work by staff with children, written consent must be gained from the child's social worker or parent/carer and placed on the child's file unless the young person is clearly of an age and understanding to give informed consent on their own behalf. Key workers must then check that consent is on the child's file before taking images. For the purpose of group activities when photography is frequently used, carers/social workers should be notified, and written consent gained using the appropriate consent form.
- 5.5.4.4 Children/young people must be clothed, and their torsos covered when being photographed or videoed. Cultural and religious traditions of clothing must be observed where needed.
- 5.5.4.5 Staff must never store or print images from their own personal devices.
- 5.5.4.6 Staff must not take any photographic images of children/young people to their own home or keep them in their private possession.
- 5.5.4.7 Photographic images of cared/ previously cared for children/young people should not be displayed in places to which members of the public have access.
- 5.5.4.8 If photos or videos are to be used for public display e.g. for publicity purposes specific permission must be sought from anyone with parental responsibility. A separate consent form will be used for this particular purpose and children must always be dressed in the images. The name of the child/young person in the image must never be used.
- 5.5.4.9 Any images of children whether stored hard copies or on disk or digitally must be stored securely.
- 5.5.4.10 Images of foster / cared for / previously cared for children must not be posted on Facebook or any other social networking internet pages.

#### 6. Personal Use of Social Media

- 6.1 It is acknowledged that many employees access social media sites outside working hours.
- 6.2 While the council does not want to impinge on the personal use of such sites, employees must be aware that inappropriate posts or blogs connected to or against the council may result in disciplinary action.
- 6.3 Employees should not have an expectation of privacy in relation to their social media content on Facebook or other content sharing platforms where it brings the Council into disrepute. Remember whilst you may have restricted your settings so that your posts can only be seen by 'Friends', content you post may be circulated more widely and accessed by others.

6.4 Employees should be aware that personal use can impinge upon their contractual relations with the Council, and they may be required to remove internet postings which are deemed to constitute a breach of this policy.

#### 7. Safeguarding

- 7.1 There are specific safeguarding issues that employees who work closely with vulnerable adults and children need to be aware of.
- 7.2 Employees with concerns or specific issues on this should raise them with their line manager in the first instance.

### 8. Use of social media in the recruitment process

8.1 Recruiting managers should not conduct searches about applicants on social media sites as this contravenes the Council's equal opportunities policy, and the recruitment and selection guidelines.

# 9. Policy Review

9.1 This policy will be reviewed by the Personnel Department and Corporate Communications Team as appropriate, in consultation with the Trade Unions and other appropriate bodies to reflect changes in employment law and developments in social media.

# 10. Monitoring

10.1 Monitoring of this policy will be undertaken in accordance with the monitoring procedures detailed in the ICT Acceptable Use Policy.

# 11. Summary

- 11.1 There are huge benefits to using social media but inappropriate use can damage the reputation of the Council.
- 11.2 As employees of Sefton Council we have a duty to ensure that any materials we publish are in no way deemed to be inappropriate.
- 11.3 Where there is evidence that an employee has misused social media and networking sites, disciplinary action will be taken in accordance with the Council's disciplinary procedure.

#### 12. Links to Other Policies

- ICT Acceptable Use Policy
- Disciplinary Procedure

#### 13. Disciplinary Action

13.1 Failure to follow this policy maybe a disciplinary matter and any breach of a-d in section 5 of this document will be viewed as potential gross misconduct.

13.2 Other violations, such as breaching the GDPR, could lead to fines being issued and possible criminal or civil action being taken against the council and/or the individual(s) involved.