

## **Social Media Policy**

### **1. Policy Statement**

The Council values the use of social media as an important way of communicating with local residents and businesses and the people who use our services. Our employees should also be able to see and have access to the Council's work on social media and should also be able to benefit from using social media for their own professional development.

The Council wishes to maximise the benefits and opportunities social media offers. The aim of this policy is primarily to safeguard both our staff and our service users while using social media, to protect the Council from the legal risks of social media, and also to ensure the reputation of the authority is protected at all times. This policy applies to employees whether they are using social media personally, on behalf of the Council, or in other ways.

### **2. Definition of social media**

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums such as Twitter, Facebook and LinkedIn. Social media also covers blogs and video and image-sharing websites such as YouTube, Instagram, Snapchat and Flickr.

Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow these guidelines in relation to any social media that they use.

### **3. Use of social media at work**

Employees are allowed to make reasonable and appropriate use of social media websites from the organisation's computers or devices, provided that this does not interfere with their duties. Employees should limit their use of social media to their official rest breaks such as their lunch break/times.

The organisation understands that employees may wish to use their own computers or devices, to access social media websites while they are at work. Employees should also limit their use of social media on their own equipment to their official rest breaks such as their lunch break/times.

In using the Council's computers or devices for private social media use, employees must be aware that in accordance with the Council ICT policies, accessing of inappropriate material is unacceptable and may result in disciplinary action.

Employees must be aware of accessing social media content on a Council PC or device which they access on their personal device but which may cause offence if it was visible or audible to others in a workplace or public environment.

#### 4. Excessive use of social media at work

Employees should not spend an excessive amount of time while at work using social media websites. They should ensure that use of social media does not interfere with their other duties. This is likely to have a detrimental effect on employees' productivity and could result in disciplinary action.

#### 5. Monitoring use of social media during work time

The organisation reserves the right to monitor employees' internet usage, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The organisation considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- Been using social media websites when he/she should be working; or
- Acted in a way that is in breach of the rules set out in this policy.

The organisation reserves the right to retain information that it has gathered on employees' use of the internet for a period of one year, or for the duration of any related disciplinary sanctions.

Access to social media websites or the internet generally, may be withdrawn in any case of misuse.

#### 6. Use of social media for work purposes

The Council has a number of authorised, managed and monitored social media feeds. **Employees must not set up or contribute to any social media activities, on behalf of the Council, without seeking advice and permission from the Marketing and Communications team first.** This is in all instances.

If you would like to request permission to set up and manage a new social media feed, you will need to provide a business case, which will be reviewed by Marketing and Communications. You will also need your manager's support and agreement. However, even with this, your request may be turned down if there is not a strong enough business case.

*If you are given permission to run a Council feed:*

Employees must be aware at all times that, while contributing to the organisation's social media activities, they are representing the organisation. Staff who use social media as part of their job must adhere to the following rules.

Employees should use the same safeguards as they would with any other form of communication about the organisation in the public sphere. These safeguards include:

- Making sure that the communication has a purpose and a benefit for the organisation;

- Obtaining permission from a manager before embarking on a public campaign using social media; and
- Getting a colleague to check the content before it is published.

Any communications that employees make in a professional capacity through social media must not:

- Bring the organisation into disrepute, for example by:
  - Criticising or arguing with customers, service users, colleagues or rivals;
  - Making defamatory comments about individuals or other organisations or groups; or
  - Posting images that are inappropriate or links to inappropriate content;
- Breach confidentiality or the Data Protection Act, for example by:
  - Revealing trade secrets or information owned by the organisation;
  - Giving away confidential information about an individual (such as a colleague or customer contact) or organisation; or
  - Discussing the organisation's internal workings (such as contracts it may be entering in to or its future business plans that have not been communicated to the public);
  - Revealing personal information about another individual;
- Breach copyright, for example by:
  - Using someone else's images or written content without permission;
  - Failing to give acknowledgement where permission has been given to reproduce something; or
- Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - Using social media to bully or harass another individual (such as an employee of the organisation); or
  - Posting images that are discriminatory or offensive [or links to such content].

Employees should not spend an excessive amount of time while at work using social media websites, even if they claim to be doing so as part of their work. If managing a feed, a campaign or an issue starts to need excessive time, you should discuss this with your manager.

## **7. Private use of social media**

The organisation recognises that many employees make use of social media in a personal capacity. While they are not acting on behalf of the organisation, employees must be aware that their behaviour can impact on the organisation if they are recognised as being one of our employees.

The organisation recognises that it is natural for its staff sometimes to want to discuss their work on social media. However, the employee's online profile (for example, the name of a blog or a Twitter name) must not contain the organisation's name.

In addition to the bullet points on page 2 and 3, any communications that employees make in a personal capacity through social media must not:

- Bring the organisation into disrepute, for example by:
  - Using the Council logo or giving the impression that you are expressing the views of the Council;
- Breach confidentiality or the Data Protection Act, for example by:
  - Revealing personal information about another individual. This includes posting photographs of service users, or commenting about service users or posting details or photographs of colleagues without their permission;

Employees should not set up vulnerable children or adults who are service users, as friends or associates.

## **8. Protecting yourself on social media**

You may wish to consider carefully who can see the information you post to social media, including your profile information, particularly employees in direct contact with service users and customers. Each social media platform offers information about how to adjust your privacy settings.

Employees and others associated with the Council should assume that anything posted on social media sites, even where privacy settings have been used, will become publicly available.

You should be aware that if you identify that you work for the Council on social media sites, this could link your behaviour outside of work to the reputation of the Council.

## **9. Disciplinary action over social media use**

All employees are required to adhere to this policy. Employees should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing

serious damage to the organisation, even if carried out in personal time or on personal feeds, may constitute gross misconduct and lead to summary dismissal.

Employees should be aware that any reports of inappropriate activity linked to the Council will be investigated. Hard copies of social media entries/web records may be used in disciplinary proceedings.

It is important for employees in politically restricted posts to remain politically neutral. Employees should therefore not express any political views, either positive or negative, on social media, or post any content that could be seen as generating or discouraging public support for a political party.

Employees should also be aware of the Code of Practice for employees when using the internet, e-mail and telecommunications, the IT Security policy, the Employee Code of Conduct and the Attendance Management Policy.

**10. Who else is covered by this policy?**

This policy applies to all employees of the Council, including those working from home or at non-Council locations.

The following groups should also have regard to this policy when working on Council business or when interacting with the Council:

- Elected Members
- Consultants
- Agency staff
- Volunteers and contractors
- External organisations (when working with the Council)

**11. Commitment to Equality**

Please identify which, if any, of the following Equality Duties this policy addresses:

<p>Eliminate unlawful discrimination, harassment and victimisation</p> <p><input checked="" type="checkbox"/></p>	<p>To advance equality of opportunity</p> <p><input checked="" type="checkbox"/></p>	<p>To foster good relations between different groups of people</p> <p><input checked="" type="checkbox"/></p>
---	--	---

One of the main purposes of the policy is to safeguard both our staff and our service users while using social media, to protect the Council from the legal risks of social media and also to ensure the reputation of the authority is protected at all times.

## 12. Related Policies

- Disciplinary Policy and Procedure
- Capability (Performance)
- Code of Practice for employees when using the internet, e-mail and telecommunications.
- IT Security Policy
- The Employee Code of Conduct
- The Attendance Management Policy

DRAFT