Social Media and Employment Policy

November 2020

TABLE OF CONTENTS

Contents

1. Policy Statement

1.1 Wyre Council acknowledges that there is significant potential for using social media and that this can bring great advantages. The responsible, corporate use of social media is therefore encouraged.

1.2 This policy provides a structured approach to using social media and will ensure that it is effective, lawful and does not compromise Council information or computer systems/networks.

1.3 Users must ensure that they use social media sensibly and responsibly, in line with council policy whether using it on council business or personal use outside working hours. They must ensure that their use will not adversely affect the council or its business, not be damaging to the council's reputation and credibility or otherwise violate any council policies.

1.4 Personal use of social media during working hours is not permitted.

2 Supporting Policies and Guidance

2.1 This Policy should be read in conjunction with the Social Media Guidance available on the Council's intranet or from the Communications Team.

2.2 This policy has links to the following policies:

- Employee Code of Conduct
- IT Computer Use Policy
- Safeguarding Children Policy
- Safeguarding Adult Policy
- Resolution Policy
- Disciplinary Policy
- Data Protection Policy
- RIPA Policy Statement

3. Definition of Social Media

3.1 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, Instagram and LinkedIn. Social media also covers blogs and video- and image-sharing websites such as YouTube, Flickr and Instagram. This list is not exhaustive.

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

4. Use of Social Media at Work

4.1 Social media will be made available for corporate / business use only.

If it is established that an employee's role should include the use of social media, approval should be sought by their Manager using the 'Social Media Access Form' from ICT, available on Topdesk.

4.2 Social media access will be granted once the request has been approved by the Communications Team and full training has been given.

4.3 Anyone wishing to set up a council related social media page, profile or group must first fill out the Social Media New Account Application Form which will need to be approved by the Communications Team. Anyone wishing to do this will need to show that the group, activity, place or event cannot be effectively promoted through the council's existing social media, and that they have the systems in place to monitor the account and reply to enquiries.

4.4 Staff who have access to council social media accounts must ensure that they are logged into the correct account and must take care not confuse them with their personal accounts. For avoidance of doubt they must not comment on or 'like' an inappropriate post (including videos) when logged into council accounts.

4.5 <u>Responsibilities of Users</u>

The following guidelines will apply to online participation and set out the standards of behaviour expected as a representative of Wyre Council.

1. Be aware of and recognise your responsibilities identified in this policy.

2. Remember that you are personally responsible for the content you publish on any form of social media.

3. Never give out personal details such as home address and telephone numbers. Ensure that you handle any personal or sensitive information in line with Data Protection.

4. Be aware of safeguarding issues, as social media sites are often misused by offenders. Safeguarding is everyone's business – if you have concerns about other site users, you have a responsibility to report these to your manager or the Designated Safeguarding Officer (see Wyre Hub for list of names).

5. Respect copyright, fair-use and financial disclosure laws.

6. Social media sites are in the public domain and it is important that you are confident about the nature of the information you publish. Permission must be sought if you wish to publish or report on meetings or discussions that are meant to be private or internal to Wyre Council. Don't cite or reference colleagues, customers, partners or suppliers without their approval.

7. Don’t use insulting, offensive or discriminatory language or engage in any conduct that would not be acceptable in the workplace. Show consideration for others’ privacy and for topics that may be considered objectionable or inflammatory.

8. Don’t download any software, shareware or freeware from any social media site, unless this has been approved and authorised by the Information Technology Team.

9. Rules apply during the period between the notice of an election and the election itself (purdah). Local authorities should not publish any publicity on controversial issues or report views of proposals in such a way that that identifies them with any individual members or political party. Full details are on the intranet and should be discussed with the Communications Team.

4.6 Investigatory Use

The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA or RIP(S)A and this includes repetitive viewing of what are deemed to be “open source” sites for the purpose of intelligence gathering and data collation.

Whilst it is recognised that social media can be used for investigatory purposes (in accordance with RIPA guidance), such as identifying fraud, illegal events, debt recovery etc. under no circumstances should employees use social media for investigatory purposes without authority from the relevant Corporate Director or Chief Executive.

Officers who have the authority to carry out investigations using social media must comply with relevant guidance and legislation. See the RIPA Policy Statement on BRIAN or available from Legal Services for further information.

5. Monitoring use of social media during work time

5.1 Social Media access is monitored in line with the guidelines set out in the ICT Computer Use Policy and staff should have no expectation of privacy when using council equipment for private usage. N.B personal use should not be in work’s time as set out in section 1.4 so should be limited to lunch breaks or before/after clocking on to work.

6. Social media in your personal life

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

6.2 Employees are allowed to say that they work for the council, and it is recognised that sometimes staff may want to discuss their work on social media. However, an employee's online profile (for example, the name of a blog or a Twitter name) must not contain the council's name.

6.3 If employees do discuss their work on social media, they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer." This does not however exempt you from the points as set out in 6.4.

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

- bring the council into disrepute, for example by:
    - criticising or arguing with customers, colleagues, Elected Members or rivals;
    - writing or knowingly confirming by liking or sharing negative, offensive or defamatory comments about individuals or other organisations or groups;
    - using foul or abusive language; or
    - posting images that are inappropriate or links to inappropriate content;
- breach confidentiality, for example by:
    - revealing information owned by the council;
    - giving away confidential information about an individual (such as a colleague or customer contact) or organisation (such as supplier or partner organisations); or
    - discussing the council's internal workings (such as its future plans that have not been communicated to the public);
- breach copyright, for example by:
    - using someone else's images or written content without permission;
    - posting anything that is copyrighted, including maps; or
    - failing to give acknowledgement where permission has been given to reproduce something; and
- do anything that could be considered discriminatory, 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 another individual (such as an employee of the council);
    - posting images or links to content that are discriminatory or offensive.

6.5 As the owner of the social media account the employee should take the necessary measures to ensure that friends or relatives do not access their social media accounts and make any posts or comments that may put the employee at detriment of this policy.

6.6 Whilst employees need to be aware of their privacy settings, restricting these does not mean that they can post what they want about the Council, individuals or organisations associated with the Council. Postings can be copied by people entitled to access them and sent on to others beyond the control of the original poster. Hence merely having privacy settings does not mean that comments will be kept out of the public domain.

6.7 Any employee who feels that they have been harassed or bullied, or are offended by material posted by a colleague on a social media site should inform their manager or a member of the HR Team.

6.8 For further information please see the guidelines – "Advice for Wyre Council employees using social media sites at home" available on Wyre Hub.

7. Use of social media in the recruitment process

7.1 Unless it is in relation to finding candidates (for example, if an employee has put his/her details on social media websites for the purpose of attracting prospective employers), the HR department and managers will conduct searches, either themselves or through a third party, on social media only when it is directly relevant to the applicant's skills or claims that he/she has made in the recruitment process. For instance, a prospective employee might claim that:

- they have used social media in their previous job (for example, as a publicity tool); or
- their social media use is directly relevant to a claim made in an application (for example, if they run a blog based around a hobby mentioned in a CV or a skill that they claim to be proficient in).

7.2 There will be no systematic or routine checking of prospective employees' online social media activities, as conducting these searches during the selection process might lead to a presumption that the applicant's protected characteristics (for example, sexual orientation or religious or political beliefs) played a part in the recruitment decision.

8. Disciplinary action over social media use

8.1 All employees are required to adhere to this and associated policies. 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, use of inappropriate language, accessing inappropriate and/or offensive channels or social media activity causing serious damage to the council, may constitute gross misconduct and lead to summary dismissal.

9. Equality Impact Assessment and Monitoring

9.1 The operation of this policy will be monitored for its impact on different equality groups in line with the Equality Act 2010. This will enable the Council to assess whether any differences have an adverse impact on a particular group, such that further action would be required.

10. Data Protection

10.1 In implementing this policy, the Council will ensure that any personal data relating to the application of this policy will be obtained, processed and destroyed in line with Data Protection requirements.