

# Social Media Policy

December 2025

## Contents

---

Contents .....	2
1. Purpose .....	3
2. Scope .....	3
3. Definitions .....	3
4. Legislative context .....	3
5. Use of social media for work purposes .....	4
6. Personal use of social media at work (including agile working) .....	5
7. Monitoring the use of social media .....	5
8. Social media in employees' personal lives .....	5
9. Use of social media in the recruitment process .....	6
10. Security .....	7
11. Breach of policy .....	7
12. Review .....	7

## 1. Purpose

---

- 1.1 This policy provides a framework for the responsible use of social media by council employees, elected members, contractors, and volunteers. It aims to:
- Promote effective, lawful, and respectful communication.
  - Protect the council's reputation and integrity.
  - Ensure compliance with legal obligations and best practice.
- 1.2 It should be used in conjunction with the [Information Security Policy](#) and the [Information Governance Framework](#) as well as communications strategies, plans and frameworks.

## 2. Scope

---

- 2.1 This policy applies to:
- All Bury Council employees, elected members, contractors, and volunteers.
  - All official Council and associated social media accounts.
  - Personal use of social media where it may impact the Council or its stakeholders.

## 3. Definitions

---

- 3.1 Social Media: Any online platform or tool that allows users to create, share, or exchange content. This includes (but is not limited to) Facebook, X (formerly Twitter), Instagram, LinkedIn, YouTube, TikTok, Threads, WhatsApp, Reddit, Snapchat, blogs, forums, and wikis.
- 3.2 Official Use: Use of social media on behalf of the Council or in a professional capacity.
- 3.3 Personal Use: Use of social media in a private capacity, not representing the Council. This also includes elected members using their own social media accounts.

## 4. Legislative context

---

- 4.1 This policy is informed by the following UK laws and guidance:
- Data Protection Act 2018 and UK GDPR – governs the handling of personal data.
  - Equality Act 2010 – prohibits discrimination and harassment, including online.
  - Employment Rights Act 1996 – protects employee privacy and rights at work.

- Local Government Act 1986 (s.2) – prohibits political publicity by local authorities.
- Defamation Act 2013 – protects individuals and organisations from false statements.
- Civil Service Code / Nolan Principles – applicable to public sector ethics and conduct.
- Contempt of Court Act 1981- the Council often promotes work to prosecute offenders (such as in flytipping cases) and / or warn and inform people in emergencies that later lead to prosecutions.
- Civil Contingencies Act 2004 – the Council is a category 1 responder and must warn, inform and advise the public so will use social media to do so.
- Copyright and intellectual property legislation – words and images used on social media channels must adhere to these to avoid fines and prosecution of the council.

## 5. Use of social media for work purposes

---

- 5.1 Employees may make reasonable and appropriate use of social media as part of their work where there is a clear benefit to use it and where other alternatives are less effective.
- 5.2 Where specific guidance is available for various forms of social media, this must be followed.
- 5.2 Employees must be aware at all times that, while contributing to the Council's social media activities (or using social media while being identifiable as a Council employee), they are representing the Council.
- 5.3 When using social media in an official capacity
  - Only authorised staff may post on behalf of the Council. Authorisation must be given jointly by the relevant Head of Service and the Head of Communications.
  - The communication must have a purpose and a benefit to the Council
  - Content must be accurate, respectful, inclusive, and politically neutral.
  - Confidential or sensitive information must not be shared.
  - All posts must comply with [accessibility standards](#) and users need to have had recent accessible standards input from the Communications team or their agreed provider of communications accessibility training.
  - Any content should be proof-read, fact checked and approved appropriately before it is published (see the [Council communications strategy](#) and standards on the intranet for approval process guidance)
  - Official accounts must be monitored regularly and moderated appropriately.
  - If you are setting up a social media account, page, profile or similar on behalf of a council service or initiative, it must be approved by the Communications team.
  - All such accounts should have resilience through more than one user having access as an administrator of the account and access being available to the Communications team.

## **6. Personal use of social media at work (including agile working)**

---

- 6.1 Employees are permitted to access the internet on the Council's equipment for personal use in their own time.
- 6.2 Personal use must be in compliance with this and any other relevant Council policies, and particularly must not involve:
  - Sharing confidential, sensitive or restricted information
  - Posting content that could bring the Council into disrepute
  - Any form of discrimination, harassment or bullying

## **7. Monitoring the use of social media**

---

- 7.1 Users of the Internet should be aware that all internet activity on Council devices is recorded. Monitoring activity is carried out in accordance with the Human Rights Act 1998 and Regulation of Investigatory Powers Act 2000.
- 7.2 Access to particular social media websites may be withdrawn in any case of misuse or changes to a particular social media platform where the platform's terms and conditions or operating model conflicts with the Council's purpose or could be considered to risk harm to our communities.

## **8. Social media in employees' personal lives**

---

- 8.1 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 Bury Council's reputation, if they are recognised as a council employee and are posting confidential information, inappropriate and/or harmful content on their personal social media.
- 8.2 Employees are allowed to say that they work for Bury Council, however, the employee's online profile must not contain the Council's name or logo. The exception for this is with professional-personal social media such as LinkedIn where the platform will automatically pull the Bury Council logo into the user's career history when they detail a period of employment here – the channel is designed for people to talk proudly about their workplace achievements.
- 8.3 Employees who wish to add information in a professional capacity to, for example a professional associations blog, should ensure it is clear that they are expressing personal views; including a simple disclaimer: for example "The views I express here are mine alone and do not necessarily reflect the views of my employer."

- 8.4 Care should be taken on the content of posts on social media, taking into consideration that posts may be brought to the attention of colleagues and senior officers if there are any concerns about content.
- 8.5 Any communications that employees make in a personal or professional capacity through social media must not:
- Bring Bury Council into disrepute by criticising or arguing with customers, colleagues, partner organisations, etc (please note, this is distinctly different to authorised colleagues rightly challenging unfair and inaccurate comments some challenging posters make on Bury Council content); making defamatory comments about individuals or other organisations or groups; posting images that are inappropriate or links to inappropriate content.
  - Breach confidentiality, for example by revealing confidential information about an individual (such as a colleague, client or customer contact) or discussing the Council's internal workings or future plans that have not yet been communicated.
  - 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.
  - Do anything that is in contravention of the Council's HR or equality policies; 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); or posting images that are discriminatory or offensive or links to such content.

## **9. Use of social media in the recruitment process**

---

- 9.1 Managers will not, either themselves or through a third party, conduct searches on applicants on social media, unless this is a requirement, for instance to ensure compliance with 'Keeping Children Safe in Education' where determining suitability to work with children. Conducting these searches during the selection process risks a challenge that an applicant's perceived protected characteristics played a part in a recruitment decision (for example, sexual orientation or religious beliefs, race - this list is not exhaustive).
- 9.2 If departments are looking to use social media as a recruitment tool, they should contact the communications team to establish scope, need and resource for job postings and/or a recruitment campaign.

## **10. Security**

---

- 10.1 Employees accessing Council emails using either their personal or business mobile phones should have the appropriate secure systems in place – with a personal device agreement in line with Information Security Policy - to ensure should their phone be lost or stolen the data cannot be accessed.

## **11. Breach of policy**

---

- 11.1 All employees are required to adhere to this policy and should consider any potential effect on the Council and/or their colleagues before posting anything on social media. Employees should note that any breaches of this policy may lead to suspension or removal of access, disciplinary action (which in the most serious cases could result in dismissal), or criminal proceedings.

## **12. Review**

---

- 12.1 This policy will be reviewed regularly by the HR Team to ensure that it is updated in line with any change in legislation.

# Document Version Control

Document Version Control	
Issue Number	Date
0.01	<<Insert>>

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.







Bury  
Council