Social Media Policy

Issued by – Communications Manager

January 2025

CONTENTS

1.0 POLICY STATEMENT

1.1 Tendring District Council (TDC) recognises social media presents opportunities to directly promote its work, share information and engage with residents, visitors and businesses, in particular through social listening (collecting feedback about the council from social media and disseminating it within the authority). However, use of social media can pose risks to our reputation as well as risks to confidential information and compliance with legal obligations.

1.2 To minimise these risks, maintain productivity of staff, ensure IT resources are used appropriately and to uphold communications standards, employees must adhere to this policy.

1.3 This policy should be read in conjunction with TDC's Social Media Guidelines and Communications Strategy documents.

1.4 This policy and the guidelines aim to promote the appropriate use of social media to further the Council's Communication Strategy and Corporate Plan objectives, and use best practice in doing so.

2.0 SCOPE OF THE POLICY

2.1 This policy covers all individuals working at all levels and grades for Tendring District Council, including contractors, sub-contractors and those otherwise working on behalf of the Council, and volunteers.

2.2 Third parties who have access to our social media accounts are also required to comply with this policy.

2.3 This policy deals with all forms of social media, including (but not limited to) Facebook, Instagram, X, YouTube, TikTok, Threads, Snapchat and LinkedIn, as well as blogs and wikis.

2.4 It applies to both business and personal use of social media, irrespective of working hours and regardless of whether or not TDC IT equipment is used to access social media.

2.5 Breach of this policy may result in disciplinary action up to and including dismissal, or in the case of contractors prompt a review of the contract.

2.6 Staff may be required to remove posts deemed to constitute a breach of this policy. Failure to comply may, in itself, result in disciplinary action.

3.0 ROLES AND RESPONSIBILITIES

3.1 The Communications Manager is the lead officer for this policy, but will work in conjunction with the Head of IT and the Human Resources department.

3.2 Corporate Directors, delegating on a day-to-day basis to Assistant Directors or Heads of Service, with a specific social media account within their area are responsible for ensuring all staff operate within the bounds of this policy, and that all staff understand and comply with the expected standards. They should also identify training needs where necessary.

3.3 All staff, including third party contractors, who use TDC social media accounts for their work are to be explicitly aware of this policy.
3.4 All staff have a duty to comply with this policy with regard to personal use.

4.0 RELATED POLICIES

4.1 This policy should be read in conjunction with the IT Strategy, Data Protection Policy, Communications Strategy, Social Media Guidelines and Branding Guidelines.
4.2 Consideration should also be given the Code of Recommended Practice on Local Authority Publicity and how it applies to social media – especially with reference to periods of heightened sensitivity
4.3 At all times thought must also be given to the Council's policy on data protection and how this will apply.
4.4 The Council's standard policies on anti-bullying, discrimination, ethical practices and confidentiality apply equally to social media as they do elsewhere.
4.5 Social media should not be used to research prospective employees of the Council, beyond the scope set out by Human Resources.
4.6 Staff should never provide references for other individuals on social media, as these can be attributed to the Council and create legal liability.
4.7 Social media should never be used in a way that breaches any of our other policies.

5.0 PERSONAL USE OF SOCIAL MEDIA

5.1 TDC recognises that employees' personal social media accounts can generate benefits to the Council, by using it to promote the Council's work, discovering content to improve how they deliver their role, and gain an understanding of community issues and opinion.
5.2 TDC also recognises employees' right to a private life; and would encourage all staff, but particularly those who are more visible (for example through regular attendance at committees or in the media), to ensure appropriate safeguards on their privacy are in place.
5.3 In accordance with the Council's IT policies, staff are able to use Council equipment to access the internet outside normal working hours. This policy also applies to the use of social media.
5.4 Employees should not engage in activities on the internet, including social media, which may bring the Council into disrepute.
5.5 Staff should not allow online activities to interfere with their day job. Unless they are using social media to directly support their work, they should only access sites (including social media) outside of their normal working hours.
5.6 The Council logo, or any sub-brands, should not be used on personal accounts.

5.7 If staff identify themselves as a Council employee on social media, they must ensure their profile and related content is consistent with how they wish to present themselves to colleagues and customers – and is consistent with this policy.

5.8 Should staff identify themselves as a Council employee in their account information, they should consider including a disclaimer that views expressed are their own; but should be aware this does not provide an exemption from compliance with this policy.

5.9 Employees must not reveal information confidential to the Council, or publish comments on their work or services offered by the Council.

5.10 Employees must not make any offensive or derogatory remarks about the Council, Councillors or other members of staff as this could amount to cyber-bullying or defamation and result in disciplinary action.

5.11 If staff use their personal account or apps to administer Council accounts, they must ensure at all times that content is posted from the correct account and that no data is downloaded to their personal devices which could constitute a breach of the Council's data protection policy.

5.12 Should an employee see content on social media which disparages or reflects poorly on TDC, they should contact their manager, the relevant service area manager, and/or the Communications Service. All staff are responsible for protecting the reputation of the Council. However, this does not mean staff should necessarily attempt to tackle or challenge such comments.

5.13 Employees are not permitted to proactively add business contacts made during the course of employment to personal social media accounts. It is at their personal discretion whether to accept invites made by business contacts to their personal accounts, but due consideration to this policy and the nature of the social media account is strongly advised in this event.

5.14 Employees should be wary of endorsements (actual, implied or accidental) of businesses or policies which the Council may consider for procurement or adoption.

5.15 Not withstanding the provisions of 5.13, it is recognised that some social media networks are designed for professional use and networking; in particular, LinkedIn.

5.16 If employees use LinkedIn and wish to share professional updates, due consideration should be given as to whether such updates would be better posted from the corporate account (and then shared); or even as a wider communications update.

5.17 Employees are encouraged to share the Council's posts on their own social media accounts.

5.18 Employees should not use their own social media accounts to conduct investigatory work for their employment; and at all times comply with the Monitoring Policy, Covert Surveillance Policy Procedure & Manual (RIPA

Policy) and other related policies and practices.

6.0 BUSINESS USE OF SOCIAL MEDIA

6.1 New social media accounts should not be set up without approval from the Head of Service, Assistant or Corporate Director, and the Communications Manager.

6.2 If your duties require you to speak on behalf of the organisation in a social media environment, you must seek approval for such communication from your manager OR the Communications Manager, who may require you to undergo training before you do so and impose certain requirements and restrictions.

6.3 Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to the Communications Manager and do not respond without approval, unless specifically tasked with dealing with such enquiries.

6.4 Staff must not post anything which could be deemed defamatory, inappropriate, or which could incur liability. If in doubt advice must be sought from a senior manager or the Communications Manager.

6.5 Staff should not broadcast personal views using the Council's social media accounts.

6.6 Employees should not post any party political content from Council accounts. Content which may be deemed 'small p' political should not be posted without extremely careful consideration.

6.7 Careful consideration must be given to copyright issues. If staff are using material protected by copyright, written consent to use such material must be obtained and kept on file, before it is posted.

6.8 Employees are expected to uphold the Council's standards for timely responses to social media enquiries as they would with a contact made to TDC by phone, email or website.

6.9 Employees are not expected to monitor or respond to social media enquiries outside of working hours, and are advised against doing so except in exceptional circumstances.

6.10 The Council will not tolerate any harassment, bullying, violent or aggressive behaviour, or discriminatory/hate crime comments towards its staff or an elected Member. The expectations it holds and the process it will take to tackle such behaviour will be posted on each channel.

6.11 Employees are not expected to tolerate abusive, discriminatory or otherwise unacceptable behaviour from social media users. Any such messages should be reported to their line manager and the Communications Manager, for appropriate response in line with Council policies.

6.12 Employees who are subjected to inappropriate behaviour on social media will be supported by the Human Resources department and associated staff support programmes.

6.13 Corporate social media accounts will only be used to conduct investigatory work if such action complies with and is duly authorised under the Monitoring Policy, Covert Surveillance Policy Procedure & Manual (RIPA Policy) and other related policies and practices.

6.14 Social media accounts should be protected by strong passwords, which are only shared with authorised users and changed when users change.

6.15 The responsible person for each account is responsible for ensuring the list of those with access is regularly reviewed and kept up-to-date; particular regard must be given to employees leaving the Council. They will be supported in this by the Communications Service.

6.16 The responsible person, a senior manager in the relevant department, and the Communications Manager, must always have full admin rights and/or passwords to accounts.

6.17 Before accessing TDC social media accounts, staff should have undergone an appropriate best practice training session, delivered by a member of the Communications Service.

7.0 MONITORING AND REVIEW OF THIS POLICY

7.1 The Communications Manager, in conjunction with the Head of IT and Corporate Resilience – and, where appropriate, the Human Resources and Council Tax Committee – is responsible for reviewing this policy every three years.

7.2 The Communications Manager, in conjunction with the Head of IT and Corporate Resilience, and the Head of People, is responsible for monitoring compliance with this policy, and its effectiveness.

7.3 TDC IT and internet resources are provided for legitimate business use, and the Council therefore reserves the right to monitor how social networks are used and accessed through these resources. Any such monitoring will only be carried out by authorised staff in line with monitoring policies

7.4 Staff are invited to comment on this policy and suggest improvements by contacting the Communications Manager.