Tendring District Council

Social Media Policy

Issued by – Communications Manager

May 2018

Bronze Award Defence Employer Recognition Scheme 2014 Proud to pledge support to the Armed Forces

INVESTORS IN PEOPLE | Gold

disability confident LEADER

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. 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 Social Media Strategy documents.

1.4 This policy and the guidelines aim to promote the appropriate use of social media to further the Council's 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, 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 Facebook, Twitter, YouTube and LinkedIn, as well as blogs and wikis.

2.4 It applies to both business and personal use of social media, whether or not within 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.

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 Regular reviews of this policy will be conducted by the Communications Manager, in conjunction with the TDC Communications Group.

3.3 Corporate Directors, delegating on a day-to-day basis to 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 the expected standards. They should also identify training needs where necessary.

3.4 All staff, including third party contractors, who use TDC social media accounts for their work are to be particularly aware of this policy.

3.5 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, Communications Strategy, Social Media Guidelines and Branding Guidelines.

4.2 At all times thought must also be given to the Council's policy on data protection and how this will apply.

4.3 The Council's standard policies on anti-bullying, discrimination, and ethical practices, confidentiality apply equally to social media as they do elsewhere.

4.4 Social media should not be used to research prospective employees of the Council, beyond the scope set out by Human Resources.

4.5 Staff should never provide references for other individuals on social media, as these can be attributed to the Council and create legal liability.

4.6 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 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.

5.3 Employees should not engage in activities on the internet which may bring the Council into disrepute.

5.4 Staff should not allow online activities to interfere with your day job. Unless you are using social media to directly support you in your work, you should only access sites outside of your normal working hours.

5.5 The Council logo should not be used on personal accounts.

5.6 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.

5.7 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.

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

5.9 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.

5.10 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.

5.11 Should an employee see content on social media which disparages or reflects poorly on TDC, contact your manager, the relevant service area manager, and/or the Communications Manager. All staff are responsible for protecting the reputation of the Council.

5.12 Employees are not permitted to 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 is strongly advised in this event.

5.13 Employees are encouraged to share Council posts on their own social media accounts.

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

6.11 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.

6.12 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.

7.0 MONITORING AND REVIEW OF THIS POLICY

7.1 The Communications Manager, in conjunction with the TDC Communications Group, the Head of IT, Head of Commercial and Customer Services and the HR Committee, is responsible for reviewing this policy annually.

7.2 The Communications Manager, in conjunction with the TDC Communications Group, the Head of IT, Head of Commercial and Customer Services and the HR Committee, 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.

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