one and all onen hag oll
CORNWALL COUNCIL

Social Media Policy

Corporate Use of Social Media for Business Purposes

19 October 2016

Customers and Communities

Summary

Headlines

The primary purpose of the 'Social Media Policy' is to clarify to employees how they should conduct themselves when using all corporately provided social media as a means of business communication and interaction for professional purposes.

The Council has set out its expectations regarding the 'Personal Use of Social Media by Employees' in the Employee Code of Conduct. If you are unclear in any way about those expectations; please ensure that you familiarise yourself with the statements for 'Personal Use of Social Media by Employees' under section 25 of the Code of Conduct for Employees as soon as possible.

All employees shall further ensure that they will not adversely affect the Council or its business, in particular, damage the Council's or its employees' reputations or otherwise breach any of the Council's policies.

Distribution

All Cornwall Council employees with access to corporate Internet resources.

Context

Background

The Council permits all employees who have accepted this policy, access to social media networking sites from Cornwall Council issued 'managed devices' such as laptops and smart phones, for business purposes only. For example, to view business related films on sites such as You Tube, or to access sites such as Facebook and Twitter to follow and gauge public opinion on a range of Council related topics.

Objectives

This policy seeks to help users of social media to make effective use of such tools for work whilst reducing risk to Cornwall Council and themselves.

Such use must however always be lawful, proportionate and must not compromise the Council's information and computer systems/networks.

Scope

Cornwall Council expects all employees, casual workers, agency workers, contractors and interim staff to comply with this policy whilst engaged on Council business.

For ease of reference the policy refers to "employees" throughout, but is intended to refer to all those listed as in scope, as above.

Details

Behavioural Use of Social Media

- In accordance with the Corporate Internet Policy, please be reminded that the Council logs and monitors all Internet usage and reserves the right to inspect any individual's activity on social media sites where there is suspected misuse. Access maybe withdrawn in any such circumstance.

- Individuals are personally accountable for postings on social media. Do not disclose information, make comments, make commitments or engage in activities on behalf of the Council unless you are authorised to do so. If you have any doubts about posting on social media in your work capacity, take advice from your line manager or the Corporate Communications Team.

- Postings on social media may attract media interest. If the media contact you directly, inform mediarelations@cornwall.gov.uk so that a suitable response can be agreed.

- Individuals accept and acknowledge that the information contained on social media sites is often subjective and that they will rely on it at their own risk.

- The Council excludes all liability, in so far as permitted by law, against any losses, claims, demands, damages, costs and expenses incurred by the individual as a result of proactively posting or responding to posts on social media sites.

- Responsible use of social media forums for professional discussion is permitted. You must however make every attempt to avoid bringing the name of Cornwall Council into disrepute or to adversely affect its reputation, customer relations or public image.

- Do not publish or link to any posts or content (text, images or video) that may result in actions for defamation, discrimination, breaches of copyright, data protection and confidence or other claims for damages. This includes but is not limited to material of an illegal, discriminatory, sexual or offensive nature that may bring the Council into disrepute.

- Social media must be used for lawful purposes only, and must comply with relevant legislation such as, but not limited to; the Criminal Justice and Public Order Act 1994, Obscene Publications Act, The Copyright, Designs and Patents Act 1998, Computer Misuse Act 1990.

- The list of circumstances which are likely to be regarded as gross misconduct (listed in the Employee Code of Conduct and the Council's Disciplinary and Capability Procedure) includes "Misuse of the Council's facilities including unauthorised use of computer, communications or

information services systems". As such, employees will be subject to a disciplinary investigation if you misuse Council systems and equipment. You may also be placing yourself at risk of prosecution if unlawful action is involved.

- Electronic communications and files are admissible in court as evidence. Do not write anything about anybody that you cannot prove and evidence. Individuals also have the right to see a copy of information held about them at any time under the Data Protection Act and the Freedom of Information Act.

- You must be vigilant towards social engineering and phishing attacks through social media in the same way as you would email. Be particularly cautious when receiving any 'direct messages' containing links. If you have any concerns that your device has become infected with a virus/malware or notice suspicious activity when or after visiting a particular social media site, please report it immediately to the Council's ICT Service Desk. .

- Council employees must not comment on or use Cornwall Council social media accounts for political purposes or specific campaigning purposes. The Council is not permitted to publish material which 'in whole or part appears to affect public support for a political party' (LGA 1986)

- Council employees must not promote personal financial interests, commercial ventures or personal campaigns through corporate social media accounts.

- Social media access from the corporate network is provided for the Council's business purposes and has an onward cost to the organisation. Whilst not explicitly prohibited, any use of personal social media accounts from the corporate network should only be used at a minimum, during breaks and at the discretion of your line manager.

Instigation and Administration of Corporate Social Media Accounts

- Any business interaction on social media must always be through one of the Council's existing corporate social media accounts that have already been approved. Information on how to contact the corporate communications team to request social media communications support is available on the intranet.

- You must not set up any new social media accounts for Cornwall Council business purposes without agreement of the relevant Head of Service and permission from the Council's corporate communications team. Whilst separate social media accounts (subject to a business case) will be considered, wherever possible we would seek to maintain a single corporate social media presence with varied daily updated content.

- Details of the process for requesting permission to set up a social media account and guidance on submitting a business case is available on the Council's intranet.

- Any social media account that is created must be administered by designated, accountable officers, as identified in the business case from the relevant service. Designated officers will be responsible for managing content, monitoring the account, setting and administering passwords to secure the account against unauthorised use. Usual good practice must apply in terms of using strong passwords which are regularly changed.

- Wherever a social media service provider offers the option of a corporate business account with the facility to create multiple and uniquely identifiable logins – this option should be used; as should any enhanced security functions such as a second factor authenticator.

- Where it is not possible to have a corporate social media account with multiple login identities, it is recognised that for both practicality and continuity purposes, the sharing of a single credential may be necessary. In such a case it is the responsibility of the designated officer(s) to ensure that the credentials are still suitably protected and shared only with those who have genuine need. Under no circumstance should this be confused with the sharing of credentials for any other corporate system which is still categorically prohibited.

- Whenever an officer leaves the organisation or moves to a role which no longer requires access to a corporate social media account, the password or other credential must be removed or changed immediately.

- All administration, updates or management of content for any corporate social media page must be conducted from one of the Council's issued managed devices. It is not permitted to log into any corporate social media account from a personally owned or non-corporately managed device. Cornwall Fire and Rescue Staff are explicitly currently exempted from this requirement only until further review. This exception is a formally accepted risk appetite decision by the Cornwall Fire and Rescue Service and Cornwall Council SIRO and will be subject to further review

Use of social media for information gathering/investigations on individuals

Whilst the use of social media is not prohibited for the purpose of investigating or intelligence gathering on specific individuals who may be subject to criminal investigation, staff must have due consideration to the Regulation of Investigatory Powers Act 2000 (RIPA), as amended by the Protections of Freedoms Act 2012. Staff must be aware that accessing an individual's social media account (without their knowledge), even on one occasion, may constitute directed surveillance and therefore such activity would require formal authorisation in accordance with Cornwall Council's RIPA Policy.

Before commencing any such activity staff should seek the necessary advice and guidance from their line manager or the Assistant Head of Governance and Information (Legal).

Management

Policy management

Authority is delegated to the Head of Governance and Information to undertake amendments of an administrative nature to this Policy as are necessary, or to secure continuing compliance with the law.

Any changes to this policy will be communicated throughout the organisation using appropriate communication channels.

This policy will be circulated via the Council's policy dissemination tool and will be available on the Information Management pages of the Intranet.

Breaches and non-compliance

Any potential misuse identified on social media websites will be reported to the appropriate officer or body. Serious breaches of this policy by Council employees will amount to gross misconduct and may result in dismissal.

Any breach of this policy which comes to the Council's attention will be investigated, and may result in action being taken under internal disciplinary and capability procedures, up to and including dismissal for actions of gross misconduct.

Please email Computer Audit if you see a breach of this policy.

How the impact of the policy will be measured

Monitor the experience of staff in using social media and how it has supported and facilitated their work via the regular staff survey. Monitor the number of breaches reported via computer audit or issues reported to Corporate Communications.

Evaluation and review

This Policy will be reviewed by the Customer and Communities Service SLT bi-annually.

Document information

Contacts

Policy prepared by Shirley Northey, Media and Digital Lead

socialmedia@cornwall.gov.uk