Social Media Policy

Version Control	
Document Name:	Social Media Policy
Version:	08032017
Author:	Director of Resources
Approved by:	Full Council
Date Approved:	March 2017
Review Date:	March 2019

Social Media Policy

1. Purpose

This Policy sets out the Council's approach to our social media presence and what are the standards expected from employees and Members when using social media. It specifies the monitoring that the Council undertakes and the actions that will be taken for any breaches.

This Policy does not form part of the terms and conditions of employment and may be amended at any time.

2. Scope

Employees and Members are expected to comply with this Policy at all times in order to observe the Council's duty of privacy and confidentiality. This Policy applies to social networking both in the workplace and personal use outside the workplace in relation to the Council and its business.

The Email and Internet Acceptable Use Policy applies to the use of social media and should be read in conjunction with this Policy.

3. Responsibilities

The Director of Resources has overall responsibility for the effective operation of this Policy and for making recommendations for any changes that will improve our social media presence as a Council and to minimise risks to operations.

All employees and Members are responsible for their own compliance with this Policy and for ensuring that it is consistently applied. It is essential that everyone take the time to read and understand it.

Employees are personally responsible for content they publish through social media – online content will be public for many years.

Members are also personally responsible for content they publish through social media.

4. How to raise a breach/concern

As a first step, employees should normally raise concerns with thier immediate line manager or their superior. This may depend, however, on the seriousness and sensitivity of the issues involved; for example if it is your line manager that has breached this policy you should approach a more senior level of management within your Directorate.

Members should raise concerns with the Monitoring Officer, Executive Director or Director of Resources.

5. Applying the policy in the workplace

a. Corporate social media

The Council's corporate social media presence will be on Facebook and Twitter, with the service specific accounts 'liked' in order to link all Council sites together. It is envisaged that the corporate accounts will be used to post information out to the public and not for conversations or blogs.

Only designated officers are permitted to post material on social media website in the Council's name. The list of designated officers and the relevant sites will be held by the Director of Resources.

News items will be posted to the Council's website, Facebook and Twitter, with links back to the main website for supplementary information. The Council's diary of events will also be posted simultaneously to the website, Facebook and Twitter.

b. Service specific social media

Where there is a business case for services to have their own social media presence, this will be presented to the Director of Resources for consideration.

Where possible, the corporate facilities should be used so that customers and followers can access all Council related information from the fewest number of sources.

c. Using work-related social media

Access to social media websites is restricted by default across the Council's network. Where work-related access is granted this does not permit employees or Members to access their personal or other interest accounts.

Before using work-related social media, employees must have read and understood this Policy, have signed the Email and Internet Acceptable Use Policy, and have sought and gained prior written approval from the Director of Resources.

d. Confidentiality

Employees and Members should never disclose commercially sensitive, anti-competitive, private or confidential information. Also, employees and Members should never upload, post or forward content belonging to a third party without that third party's consent.

e. Third Parties

Before posting a link to a third party website, check that any terms and conditions of that website permit you to link to it. All links must be done so that it is clear to the user that they have moved to a third party's website. When making use of any social media platform, employees must read and comply with its terms of use. Employees and Members will not post, upload, forward or post a link to a chain mail, junk mail, cartoons, jokes or gossip.

f. Personal use of social media websites

The Council does not permit the personal use of social media websites through its computer systems/networks in any circumstances. Any use of social media websites using personal devices while in the workplace must never interfere with work effectiveness and must comply with personal use restrictions in the Council's Email and Internet Acceptable Use Policy

6. Social media in your personal life

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

Employees are allowed to say that they work for the Council and their online profile may contain the Council's name. However, omitting the Council from their online profile does not remove the expectation that friends and family will know that the person's paid employment is with the Council. This also applies to Members.

Employees and Members should always remember that any information disclosed through personal accounts on social networking sites is disclosed in a personal capacity, and never on behalf of the Council. Where employees and Members disclose their association with the Council through social media used for personal purposes, any views they publish should be presented as purely personal views rather than being representative of the views of the Council.

Employees and Members must also bear in mind their audience when posting on social media sites. They should ensure that those who are able to access the information they post have a right to see it and also that it is appropriate that they see such information.

Employees should be aware that the Officers' Code of Conduct covers the issues of standards and information disclosure and should always bear this in mind when using social media in a personal capacity. The Members have their own Code of Conduct.

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

- breach confidentiality, for example by: revealing confidential intellectual property or information owned by the Council or;
- give away confidential information about an individual (such as a colleague or customer) or organisation (such as a contractor or supplier); or
- discuss the Council's internal workings (such as agreements that it is reaching with contractors/customers or its future plans that have not been communicated to the public) or;

- present the Council as a bad employer or criticise the Council, directly or indirectly;
- do anything that could be considered discriminatory against, 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 or;
- use social media to bully another individual (such as an employee of the Council) or;
- post images that are discriminatory, offensive or inappropriate, or links to to such content, for example:
    - anything illegal;
    - any kind of pornography;
    - show or incite abuse, violence, hate or discrimination;
    - promote gambling, drugs or alcohol abuse; or
- bring the Council into disrepute, for example by: criticising or arguing with customers, colleagues, contractors etc. or;
- make defamatory comments about individuals or other organisations or groups or;
- fail to give acknowledgement where permission has been given to reproduce something.

The various social media feeds such as Facebook, Twitter and Instagram, all have different ways of allowing users to support the message of a post, tweet or photo etc. Communications that breach these guidelines do include likes, retweets or hearts etc., of posts, tweets or photos etc.

All employees and Members are required to adhere to these guidelines. Employees should be aware that use of social media in a way that may be deemed as deliberate or inadvertent misuse which could be a breach of these guidelines, may lead to disciplinary action under the Council's Disciplinary Procedure. Serious breaches of these guidelines, for example incidents of bullying of colleagues or social media activity causing serious damage to the Council, may constitute gross misconduct and may lead to action under the disciplinary procedure up to and including dismissal.

Misuse of social media can, in some circumstances, constitute a criminal offence or otherwise give rise to a legal liability against the individual and the Council. Any such action will be addressed under the Council's disciplinary procedure and is likely to result in dismissal.

7. Monitoring social media

The Office of Surveillance Commissioners is responsible for overseeing the use of covert surveillance by designated public authorities based in the United Kingdom.

The Office of Surveillance Commissioners' view is that the repeat viewing of individual "open source" sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA authorisation provides.

The Protection of Freedoms Act 2012 (in particular a statutory instrument made under the Act) restricts the use of RIPA to conduct that would constitute a criminal offence which is punishable by a maximum custodial sentence of 6 months or more. This effectively restricts the use of RIPA to circumstances when the conduct is considered to be serious criminal conduct, by reference to sentencing powers.

The Council does not engage in monitoring social media outside of the Regulation of Investigatory Powers Act (2000). See the Surveillance Policy for more details on the requirements of any RIPA application.