Information Security
Social Media Policy

Version: 2.7
Published: 29 September 2022

Document Control

Related Documents

Title	Author	Version & Date

Revision History

Release Date	Revision Version	Summary of Changes
22/11/2012	V1.0	Standardisation and issue
01/09/2015	V2.0	Revised and layout updated
01/09/2016	V2.1	Updated
01/09/2017	V2.2	Reviewed
01/09/2018	V2.3	Updated for GDPR and DPA2018
01/09/2019	V2.4	Reviewed
12/12/2019	V2.5	Authorised signatory added
29/01/2021	V2.6	Reviewed
05/08/222	V2.7	Reviewed. Information Governance Group replaced by SIRO Performance Review Group

Reviewed By
This document (or component parts) has been reviewed by the following:

Name or Group Name	Revision Version	Approval Date
Information Security Officer	V1.0	21/11/2012
Information Security Officer	V2.0	01/09/2015
Information Security Officer	V2.1	01/09/2016
Information Security Officer	V2.2	01/09/2017
Information Security Officer	V2.3	01/09/2018
Information Security Officer	V2.4	01/09/2019
Information Security Officer	V2.5	12/12/2019

Information Security Officer	V2.6	29/01/2021
Information Security Officer	V2.7	05/08/2022

Document Approval
This document requires the following approvals:

Name or Group Name	Revision Version	Approval Date
Information Security Officer	V1.0	21/11/2012
Information Security Manager	V2.0	01/09/2015
Information Security Manager	V2.1	01/9/2016
Information Security Manager	V2.2	01/09/2017
Information Security Manager	V2.3	01/09/2018
Information Security Manager	V2.4	01/09/2019
Information Security Manager	V2.5	12/12/2019
Information Security Manager	V2.6	29/01/2021
Information Security Manager	V2.7	05/08/2022

Authorised Signatory

Senior Information Risk Officer (SIRO)	V2.5	22/01/2020
AD Organisational Change (Deputy SIRO)	V2.6	
AD Organisational Change (Deputy SIRO)	V2.7	28/09/2022

Contents

1 Introduction

'Social media' is the term commonly given to websites, online tools and other Information Communication Technologies (ICT) which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests. As the name implies, social media involves the building of communities or networks, encouraging participation and engagement.

The use of social media presents new and interesting opportunities for the Council to reach out to its residents and service users. Social media enables anyone with a computer and internet connection the quick and easy ability to publish opinion and information, and listen to and engage with those who read it.

This presents exciting opportunities for organisations to have conversations with the wider community in order to share news, information on services, and seek opinions from those with whom they work and serve.

Alongside these opportunities it must be recognised that there are risks attached to the use of social media. Distribution of material cannot be controlled. Once posted to an initial target audience, material can be posted anywhere through the networks of each individual in that audience and beyond. It is therefore important that users of social media understand the pitfalls as well as the benefits of the technology.

This policy has been introduced to ensure appropriate, legal and effective use of social media as a communication channel for Cumbria County Council. It will interact with other Council policies in this area of work, including the Corporate Communications Strategy, the Visual Brand and Communications Guidelines, the Standard for Information Security and other relevant Policies.

The aims of this policy are:

- to protect the reputation of the County Council and
- to prevent the unauthorised use of County Council branding on employees' personal social media sites.

2 Responsibilities

The Senior Management Team is responsible for ensuring that employees are aware of their work-related and personal responsibilities.

The SIRO Performance Review Group will review and revise this policy and procedure as appropriate.

All managers are responsible for ensuring that their staff understand this policy and abide by it, and for giving guidance where employees are unsure of appropriate content for use on social media sites.

HR Advisers are responsible for advising and supporting managers in the application of the policy.

All employees, temporary and contract workers, and members of Cumbria County Council are responsible for complying with this policy.

3 Applying This Policy

3.1 Council-run channels

County Council staff considering the use of, or wishing to use, social media as a channel for a project or campaign MUST refer to the Visual Brand and Communications Guidelines – Social Media Protocols which can be found on Intouch.

This protocol is designed for Members, senior managers and staff to ensure that Cumbria County Council gives full consideration to its online engagement and participation activities in order to maximise the potential and minimise the risk of engaging in this way, both for the individual and for the council.

3.2 Personal use of social media channels

Individuals employed by the council are entitled to use whatever system they like outside of their working time and working persona, to engage in the social aspects of the media – both broadcasting and receiving. However great care should be taken to ensure the private/work line is not crossed.

It is good practice to follow the stricture of never mentioning work, opinions of colleagues or processes and projects on private Social Media Networks – this also includes not divulging information that is then posted by family, partners and friends.

It is essential employees do not identify themselves as a 'professional' (for example Social Worker or Occupational Therapist and then give personal comments. This may be interpreted as professional based comments and may bring a wider profession into disrepute; this may be against the professional code of practice (regardless of the profession) and could result in action from the registration body

If employees have listed their general role within an organisation (for example on a ‘Profile Page’, it is important they:

- Do not engage in activities on the internet that might bring the Council into disrepute.
- Do not use the Council logo on personal web pages.
- Do not reveal anything which may directly or indirectly compromise the Council, its Service Users or employees – examples of this can be: Comments (or information) about current work/projects, information that can directly or indirectly identify a service user. If an employee needs to ask themselves whether something is appropriate, it probably isn’t.
- Where possible do not accept service users or ex-service users as ‘friends’/’followers’ or ‘contacts’ on your site. This may cause a conflict of interest or even breach certain professional codes of conduct. If in doubt – stop.
- Do not include contact details or photographs of service users or staff without their explicit permission.
- Under no circumstance should offensive comments be made about any person. This may amount to cyber-bullying or defamation and could be deemed a disciplinary offence. (Please note that comments made from a personal perspective may still bring the Council into disrepute).

4 Reporting Breaches

All Social Media information breaches will be managed in line with the Cumbria County Council Information Security Incident Management Policy.

All Information Security Standards, Policies and Procedures are available on InTouch.

5 Appendix 1 – Social Media

5.1 Definition

'"A social network service focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web-based and provide a variety of ways for users to interact, such as e-mail and instant messaging services.
Social networking has encouraged new ways to communicate and share information. Social networking websites are being used regularly by millions of people.' (source: Wikipedia).

Any site that allows the interaction between people and/or organisations can be considered social networking, though most people think of Facebook and similar sites as typical examples of social networking.

5.2 What does a social networking site do?

These sites provide a platform – typically outside of an organisation's network – typically based on the World Wide Web where anybody can gain access and interact in some way with others. That interaction can be mainly written, as in Facebook and Twitter, it can be video as in YouTube or it can be multimedia, as in MSN. The main reason is often to keep in touch with larger groups of people already known to you, such as school or university friends.

Internal Social Media systems exist and the County Council is exploring that possibility at present. The difference being 'Internal' means the content is not available to the outside world. It is a locked system.

5.3 What is a blog?

A blog is a form of diary or mini web site – usually web hosted and available to the world, although corporate and closed systems using blogs also exist. Open blogs are universally available and searchable and are mainly constructed by individuals to talk about issues which interest them.

Blogs cover the whole spectrum of human activity and are the ultimate niche communication/marketing tool. Anybody can set one up using the likes of blogger.com or Wordpress.com. It takes just a few seconds.

6 Appendix 2 - Legal Issues

6.1 General

There are circumstances under which employers can be held legally responsible for online content published by their employees. This may include action taken as part of their role for the organisation and material published on official organisation channels or somewhere that has been previously sanctioned by the company. It is therefore important to make all employees aware of the potential legal issues as well as any specific company policy on engaging with social media.

Giving employees clear guidelines on what is and isn't considered acceptable helps both parties to understand the parameters when dealing with social media from an employment perspective. If using an organisational blog, we should bear in mind that posting the opinions of others can mean assuming a certain amount of legal responsibility for the content. We should therefore include a policy on any council blogs that outline how comments will be treated (for example, comments may be reviewed or moderated before publication).

It is important that employees are aware that posting information about the Council can not be isolated from their working life. Any information published online can be accessed around the world within seconds and will be publicly available for all to see.

Employees should take the following into consideration when using social media:

- Be aware of the Council policy and guidelines for using social media, whether this is for personal use or as a part of their working role.
- Be familiar with the legal areas outlined below before writing about colleagues or sharing information about the Council.
- Ensure that posted material does not disclose privileged or confidential information.
- Examples of social media activities outlawed under the Consumer Protection from Unfair Trading Regulations:
- Creating fake blogs ('ghosting').
- Falsely representing oneself as a customer.
- Falsely advertising on social media sites.

6.2 Libel and defamation

Defamation is the act of making a statement about a person or company that is considered to harm reputation, for example, by lowering others' estimation of the person or company, or by causing them to lose their rank or professional standing. If the defamatory statement is written down (in print or online) it is known as libel. If it is spoken, it is known as slander. There are exceptions to this - posting a defamatory statement online or recording it on a podcast would both be examples of libel.

6.3 Other points to note

An organisation may be held responsible for something an employee has written or said if it is on behalf of the company or on a company-sanctioned space. Action can also be taken against anyone repeating libellous information from another source, so careful checks are needed before quoting statements from other blogs or websites. This can also apply to linking to defamatory information.

You should consider whether a statement can be proved before writing or using it – in law, the onus is on the person making the statement to establish its truth.

An organisation that provides a forum for blogging can be liable for defamatory statements they host.