Organisation	Somerset County Council
Title	**Internet & Social Media Policy**
Author	Peter Grogan
Owner	Information Governance Manager
Security Classification	OFFICIAL-Unclassified

POLICY ON A PAGE

This policy provides information on the use of the Internet and social media, both professional and personal use, the rules and guidance that must be followed, the standards to be maintained, the risk to users, customers and the Council and the potential consequences of misuse.

Somerset County Council will ensure that all users of the Internet and social media, both professional and personal, are aware of the rules and responsibilities associated with this use.

This document will be distributed to: **All Elected Members, Somerset County Council Staff, 3rd Party Contractors, Secondees and Volunteers**

Key Messages

- SCC encourages the responsible, professional use of the Internet and social media to support service delivery and professional development.
- Users must always adhere to the Information Governance Policy framework that includes Data Protection, Acceptable Use and associated guidance.
- Respect copyright, fair-use and financial disclosure laws. Don't download any software, shareware or freeware from the internet unless this has been authorised by Information Services (IS).
- Any social media or Internet developments by services are considered publications, and must be developed in line with the SCC Social Media Handbook and receive approval prior to development by the Corporate Publications Panel.
- Be aware of safeguarding, radicalisation issues and fraud, as social media sites can be used to target the vulnerable. You have a responsibility to report any safeguarding and radicalisation issues to the lead officer in your service and comply with related legislation and attendant investigations.
- The Council's Internet connection is intended for business use. Limited personal use of the Internet by employees as defined within this policy is acceptable. To protect your personal security you are advised not to use banking or shopping over the SCC internet connection.
- The Council recognises an employee's right to a private life. However you must also ensure the reputation and confidentiality of the Council are protected. Don't cite or reference customers, colleagues, partners or suppliers without their approval.
- Cyber-bullying or harassment is unacceptable and managers must take appropriate action to deal with such events in accordance with the SCC Dignity at work policy.

This "policy on a page" is a summary of the detailed policy document please ensure you read, understand and comply with the full policy

Revision History – to be revised annually from publication date

Revision Date	Editor	Previous Version	Description of Revision
01.07.11	Peter Grogan		Initial Draft
22.12.12.	Peter Grogan	v.11	Complete rewrite
20.03.13	Peter Grogan	v1.0	HR Amendment (Appx 1)
23.12.13	Peter Grogan	v1.1	Addition of Banking & Shopping Paragraph
01.01.15	Peter Grogan	v2.0	EGRESS and new security classification
05.10.15	Peter Grogan	v2.1	PREVENT radicalisation update

Document Approvals

This document requires the following approvals:

Approval	Name	Date
Information Governance Manager	Peter Grogan	
SIRO	Richard Williams	
SCC HR	Vicky Hayter	
Unions / JCC	[redacted]	

Document Distribution

This document will be distributed to: **All Elected Members, Somerset County Council Staff, 3rd Party Contractors, Secondees and Volunteers**

FULL POLICY DOCUMENT

1 Policy Statement

Somerset County Council will ensure that all employees engaging in the use of the Internet and social media, both professional and personal, are aware of the rules and responsibilities associated with this use.

2 Purpose

The purpose of this policy is to outline the responsibilities of employees of Somerset County Council using the Internet and social networking sites and should be read in conjunction with the Council's other related Information Governance and HR policies.

The Internet and social media offer great potential for improving communication, information collection, publicity and building relationships with service users and partners and improving the services that we provide.

The purpose of this policy is to ensure:

- Successful delivery of services through the internet and social media.
- Those services represent good value for money.
- A consistent and corporate approach in the use of the internet and social media.
- That information remains secure and is not compromised.
- That users operate within existing SCC policies, guidelines and relevant legislation.
- That users are protected, and managers are supported.
- That the Council's reputation is not damaged or adversely affected.

3 Scope

This policy applies to all employees and elected Members and other workers (including casual and agency workers, volunteers, secondees and contractors) who use the Council's infrastructure and are granted access on the above grounds.

This policy does not apply to schools and users that are not included in the paragraph above. Such users must comply with their own policies on social media use.

It is acknowledged that there is significant potential for Somerset County Council to exploit the Internet and social media and that this can bring great advantages. The responsible, corporate use of both the Internet and social media is actively encouraged.

Any personal information dealt with over the internet or in social media must be dealt with in accordance with the Data Protection Act 1998.

4 Definition

This policy provides a structured approach to using the Internet and social media and will ensure that it is effective, lawful and does not compromise the Council's reputation, Council information or computer systems.

The Internet and social media encourage interaction where people are talking, participating and sharing online. They combine to deliver and exchange information and allow users to participate in the creation and development of the content.

Social media includes (but is not limited to) Facebook, Twitter, Linkedin Youtube, Flickr and Google+. The terms 'social media' and 'social networking' are interchangeable terms that cover every form of communication and interaction between people online.

5 Risks

Somerset County Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

Examples of the potential risks are:

- Loss or theft of personal data
- Virus or other malware (malicious software) infection from external sites.
- Disclosure of confidential information.
- Damage to the reputation of the Council.
- Social engineering attacks *(this is the act of manipulating people into disclosing confidential material or carrying out certain actions. Social engineering is often conducted by individuals fraudulently claiming to be a business or client).*
- Civil or Criminal action relating to breaches of legislation.
- Employees using sites to bully or harass other employees
- Degradation of network bandwidth due to media streaming and downloading.

In light of these risks, the Council regulates the use of the Internet and social media sites to ensure that such use does not damage the Council, its employees, partners and the people it serves.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6 Applying the Policy

6.1 User Responsibilities

If a user accesses any information and communications technology, including email and social networking sites, to make reference to people working at or for the Council, or people receiving services from the Council, then any information posted must comply with the Council's Standards of Conduct, any relevant Professional Codes of Practice, and the Corporate Information Security Policy.

Any Internet or social media developments by Services are considered publications, and must receive approval prior to development by the Corporate Publications Panel.

When designing, developing and delivering a social media presence Services are required to do so in line with the SCC Social Media Handbook.

Services considering, or in the process of, developing a social media presence can obtain support from the Communications Team, who will be able to provide advice and guidance including lessons learnt from other services.

6.1.1 Monitoring

The Council continuously monitors Internet and email use by electronic means Surveillance & Monitoring Policy, and users cannot expect privacy when using the Council's Internet facility. Monitoring will include volume of Internet traffic, the internet sites visited, type of site and length of time of any visit to a site.

All monitoring will be undertaken in accordance with the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 and the Regulation of Investigatory Powers Act (2000).

Email and internet history will only be accessed as a result of a direct request from a senior manger as a result of reasonable concerns over misconduct.

6.1.2 Content filters

The Council does not wish to limit freedom of expression or act as a censor but in acting as arbiters of what is "reasonable" certain websites will be blocked by the web filters.

- Pornography
- Gambling
- Violence
- Weapons
- Illegal activity

All users are advised that access to these sites is blocked. If you require access to a blocked site for, professional reasons, please contact the Information Governance Manager for advice.

Users who accidentally or unintentionally access a site containing any prohibited content should leave the site immediately and inform their line manager. Genuine mistakes and accidents will not be treated as breach of this policy

6.1.3 Offensive Material

Users are not permitted to access, transmit, display or download from Internet sites that hold offensive material. Offensive material includes, but is not restricted to, hostile text or images relating to:

- gender,
- race or ethnicity,
- sex or sexual orientation,
- religious or political convictions
- disability
- material that is designed or would annoy, harass, bully or cause anxiety to others

The Council is the final arbiter on what is or is not offensive material or what is or is not acceptable, permissible or excessive use of the Internet – users concerned about this should refrain from using the Internet for personal use.

6.1.4 Spam, Phishing and Unsolicited mail

Users must not forward or distribute any unsolicited commercial web mail, chain letters or advertisements, or any email or message which purports to give a safety or security warning, unless that message comes from the Council's Communications team. External warnings of this kind should be forwarded to ICT for verification.

6.1.5 Limitations on Copyright and unlicensed performance

Users must not download or use digital media including music, images, photos and video which would be in breach of copyright or licensing arrangements, or where copyright or ownership can not be determined.

6.1.6 Personal data and sensitive business information

Users must not communicate personal or business sensitive information over the Internet/Intranet for any purpose, unless authorised to do so.

Never give out personal details such as home address and telephone numbers. Ensure that you handle any personal or sensitive information in line with the Council's Data Protection Policies.

Employees should be aware that the Employees' Code of Conduct covers the issues information disclosure, and should bear this in mind when using social media (in a personal capacity) outside of work. Employees should be aware that any reports of inappropriate activity, linking them to the council, will be investigated under the Councils **Surveillance and Monitoring Policy**

With the rise in identity theft and fraud, employees may wish to consider the amount of personal information that they display on their personal profile.

6.1.7 Use of Hardware and Software

Users are not permitted to:

- download software from any source without approval from IT services
- alter or tamper with their PC Internet settings for the purpose of bypassing or attempting to bypass filtering and monitoring procedures
- use unauthorised file sharing and torrent services.

6.1.8 Use of cloud Storage

The use of cloud storage e.g. Google Drive, Dropbox, SkyDrive, iCloud is prohibited other than in approved circumstances. Access to cloud storage is prevented in order to prevent data storage or handling in breach of the Data Protection Act and to prevent malware entering corporate networks.

Access to cloud storage by third parties to download business data may be granted for legitimate business use where appropriate safeguards are in place. Please contact Information Governance for further information.

6.1.9 Radicalisation – PREVENT

Online radicalisation is an ever increasing issue through social media which can include accessing inflammatory material or online grooming. This can affect even the most remote rural areas who may never have witnessed any extremism previously. The Prevent Duty is therefore a key area of focus for internet and social media protecting people from being drawn into terrorism. You have a statutory responsibility to report any safeguarding issues to the lead officer in your service and comply with related legislation and attendant investigations.

6.2 Using the Internet and social media – for work purposes

There is significant potential for using the Internet and social media to deliver services. Services must ensure that they use the Internet sensibly and responsibly, in line with corporate policy and that their use will not adversely affect the Council or its business, nor be damaging to the Council's reputation and credibility or otherwise violate any Council policies.

Use of the Internet and social media by the Council should be able to clearly demonstrate one or more of the following:

- Improved customer experience. e.g. better engagement, response times, availability etc

- Reduction in the cost of delivering a service
- There are sufficient resources to support and regularly update

When using the Internet and social media on behalf of the Council the material published must:

- have prior approval from the Corporate Publications Panel
- be truthful, objective, legal, decent and honest
- comply with all of the requirements of the Data Protection Act 1998, and must not breach any common law duty of confidentiality, or any right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information
- be respectful and professional at all times, and material must not be couched in an abusive or hateful manner
- be in line with the Council's Staff Code of Conduct, and must not breach the Council's Dignity at Work Code of Practice.

When using social media on behalf of the Council the material published must not:

- breach copyright
- risk actions for defamation, or be of an illegal, sexual, discriminatory or offensive nature
- be for party political purposes or specific campaigning which in whole or part appears to affect public support for a political party
- be used for the promotion of personal interests or commercial ventures or campaigns

Where individuals from partner organisations contribute and are acting on behalf of the Council, they must comply with relevant Council policies

Personal social media accounts may be used where a personal account is required to access a business account such as Facebook or for the use of professional networks to conduct council business with customers/clients. When linking a personal account to a business account, users should exercise appropriate caution and always be aware of which account they are posting from.

If an employee receives any threats, abuse or harassment from members of the public through their use of social media then they must report any such incident to their line manager.

6.3 Training and Professional use of Internet and social media

The responsible, professional use of the Internet and social media to support service delivery or professional development and training is viewed positively. If you have any issues accessing professional training resources from providers please contact the ICT helpdesk.

6.4 Personal use of Internet and social media

The Council's Internet connection is intended for business use. Limited personal use of the Internet by users before and after their working hours and during official rest breaks is acceptable provided that the material accessed is appropriate, is consistent with the Council's code of conduct and Dignity at Work Code of Practice, and does not adversely impact on the use of the facilities for business purposes.

6.4.1 All users

There is no right for users to use the Internet for private use and access can be withdrawn at any time, all users must be aware that if the internet is used for personal use:

- The Council is not liable for any personal financial or material loss
- Inappropriate or excessive use may result in removal of Internet facilities

- Due to the potential impact on business systems, the personal use of streaming media such as video (YouTube, BBC iPlayer, Vimeo etc.) or audio (internet radio, Spotify, Google Music etc.) outside work hours should be kept to a minimum. Streaming should be limited to occasional short video/audio clips only. You must not stream TV, films or continual broadcasts (e.g. sport, news, radio or playlists)
- Due to the potential impact on business systems, the downloading of media for personal use such as video (YouTube, BBC iPlayer, Vimeo etc.) or audio (internet radio, Spotify, Google Music etc.) is not permitted.

6.4.2 Employees

In addition employees should be aware that

- Inappropriate or excessive use may result in disciplinary action.
- If you wish to spend significant time using the Internet in working hours – e.g. for study purposes – you must obtain approval from your line manager.

Managers and Employees should remember that this document should not be read in isolation, instead it should be used in conjunction with related policies and guidance as listed under Appendix 1 at the end of this policy.

6.4.3 Banking and Internet shopping

Whilst the Council does permit access to a variety of sites on the internet, via SCC network, the Council cannot guarantee the security of banking details, logins and passwords to your personal shopping or subscription accounts. The Council therefore advises you do not access these services on the Council network.

6.5 Council reputation and confidentiality

The Council recognises an employee's right to a private life. However the Council must also ensure its reputation and confidentiality are protected.

Therefore any user accessing the Internet and social networking sites for work purposes must:

- refrain from identifying themselves as working for the Council, in a way which has, or may have, the effect of bringing the Council into disrepute;
- not express a personal view that the Council would not want to be associated with;
- notify the Communications Team if the content posted conflicts with their role in the Council.
- take care not to damage relationships with work colleagues, partner organisations, elected members, clients or service users.

6.6 Acceptable use by the public - moderation

Where a council service uses social media, it must be able to moderate the content of posts by the general public in order to protect individuals, council employees, as well as the reputation of the Council. Any use of the Council's social media must be in line with the Moderation Policy. Services will be expected to provide resource to enforce the policy.

Appendix 1

Governance Arrangements

7 Policy Compliance

If an employee is found to have breached this policy, they may be subject to Somerset County Council's Disciplinary procedure. Where it is considered that a criminal offence has potentially been committed, the Council will consider the need to refer the matter to the police.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Information Governance team.

Policy Governance

The following table identifies who within Somerset County Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Information Governance Manager
Accountable	SIRO - Director of Business Development
Consulted	Senior Management Team, HR, Unions
Informed	All, Members, employees, contractors, volunteers and 3rd parties.

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. Policy review will be undertaken by the Information Governance Manager.

References

The following Somerset County Council policy documents are directly relevant to this policy, and are referenced within this document:

- Corporate Information Security Policy
- Data Protection Policy
- Acceptable Use Policy
- Legal Responsibility Policy
- Dignity at Work – Code of Practice
- Managers guide to Cyber-Bullying / Harassment
- Employee guide to Social Media / Networking
- Moderation Policy