SURREY HEATH BOROUGH COUNCIL

SOCIAL NETWORKING POLICY

April 2022

Surrey Heath Borough Council
Knoll Road, Camberley GU15 3HD
Data.protection@surreyheath.gov.uk

Contents

1. Introduction

The main purpose of the Social Networking Policy is to provide guidelines for the effective and safe use of social networking to promote and develop Surrey Heath Borough Council's (SHBC) services, and to ensure employees and workers are aware of how they should conduct themselves when using social networking sites both at work and outside of work. There are also specific safeguarding issues that employees or workers who work closely with children or vulnerable adults need to be aware of. Please refer to the SHBC Safeguarding Policy for more information.

The Council are committed to making the best use of all available technology and innovation to improve the way we do business, this includes embracing social networking. The Council is pro social networking. However, we have a responsibility to ensure it is used appropriately by all.

2. Definitions

The term 'social networking' is given to websites, online tools, apps and other ICT which allow users to interact or collaborate with each other either by sharing information, opinions, knowledge and interests. The term 'Blogs' refer to online diaries. Other platforms include message boards, podcasts, social networking (such as Twitter, Facebook, Instagram, WhatsApp and Snapchat) content sharing websites (such as YouTube, Slack, and Flickr) and web conferencing sites such as Zoom and MS Teams.

3. Scope

The Social Networking Policy will apply to all employees and workers (including fixed term, casuals, agency staff, contractors and work experience students, volunteers as well as permanent staff) employed on Council business, including those working with partner organisations. This policy should be read in conjunction with the following policies and all other relevant policies will apply:

- Information Governance Strategy and Policy
- Information Security Policy
- Data Protection Policy
- Disciplinary Policy
- Code of Conduct for Officers
- Bullying and Harassment Policy
- Communication guidelines
- Speak Up Policy
- Safeguarding Policy
- Mobile Phone Agreement
- Vexatious and Persistent Complaints Policy and Procedures

The Council reserves the right to conduct investigations where a breach of the Social Networking Policy is suspected. Breach of this policy may be dealt

with under the council's disciplinary policy. Serious cases may be treated as gross misconduct leading to dismissal.

Misuse of social networking websites (both inside and outside of work, if work information is involved) can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against the individual responsible for the content and/or the council.

4. Policy Statement

The Social Networking Policy covers all forms of social networking which include (but are not limited to):

- Facebook, Instagram, Snapchat, Nextdoor and other social networking sites
- Twitter, WhatsApp, discussion forums and other blogging sites
- YouTube and other video clips and podcast sites
- Zoom, MS Teams and other web conferencing sites
- LinkedIn
- All forms of collaborative tools including Slack, Trello and Chatter

5. Equality Assessment

The Council's equality scheme demonstrates its commitment to equality internally and externally and ensures that all sections of the community are given an opportunity to contribute to the wellbeing of the community. An equality impact assessment has been carried out on this policy and procedure.

The Council ensures that consultation is representative of the community and that consideration is given on how to consult hard to reach groups and will positively learn from responses.

6. Principle and Aims

6.1 The Council recognises that social networking is an effective communication mechanism which can be used alongside other communication methods. This policy is not intended to restrict employees and workers from using social networking at work and at home, but to make them aware of the risks they could potentially face with how they share information.

6.2 To ensure that when social networking is used to communicate with the public, stakeholders and partners by all SHBC staff in the performance of their duties, that it is, aligned to the Council's communication guidelines.

6.3 To ensure that the reputation of SHBC is protected and the Council is not brought into disrepute.

6.4 To ensure that any SHBC communication through social networking meets legal requirements.

6.5 To ensure that all SHBC social networking sites are easily identifiable as originating from the Council and correctly apply the Council's logo according to brand guidelines.

6.6 To prevent the unauthorised use of Council branding on employee or workers' personal social networking sites.

6.7 To ensure that SHBC employees and workers are aware of cyber-bullying and defamation and that this would be deemed as a disciplinary offence and/or a criminal offence.

6.8 To ensure inappropriate language is not used on any SHBC presences or posts, and SHBC core values are considered at all times

6.9 To ensure content remains professional at all times.

7. Policy and Procedure

7.1 If employees and workers make reference to the Council on a personal internet site, they should follow these guidelines:

- Do not engage in activities over the internet that could bring the Council into disrepute.
- Do not use the Council logo on personal web pages.
- Do not reveal information which is confidential or sensitive to the Council – consult your manager if you are unsure. Do not discuss existing or proposed policies on social networking websites.
- Do not include contact details, personal details or photographs of service users or staff without permission.
- Do not make offensive comments about the Council, members, colleagues, suppliers or residents of Surrey Heath on the Internet. This may amount to cyber-bullying or defamation and could be deemed a disciplinary offence and/or a criminal offence.
- Do add a disclaimer to your profile stating that opinions are your own.
- Personal accounts should not be used to comment on Social Media postings regarding SHBC on behalf of SHBC. For a consistent response employees and workers should notify the Marketing and Communications Team for Council-related postings.

7.2 If employees and workers create a social networking site from Surrey Heath Borough Council, they should follow these guidelines:

- Do not engage in activities over the internet that could bring the Council into disrepute.
- Do not reveal information which is confidential or sensitive to the Council – consult your manager if you are unsure.
- Do not discuss existing or proposed policies on social networking websites.
- Do not include contact details or photographs of service users or staff without permission.
- Do not make offensive comments about the Council, members, colleagues, suppliers or residents of Surrey Heath on the Internet. This may amount to cyber-bullying or defamation and could be deemed a disciplinary offence and/or a criminal offence.

- Ensure naming conventions remain professional and where linked to an individual, forename and surname combination should be used

7.3 If employees and workers are considering any social networking campaigns they should firstly consult the Marketing and Communications Team for guidance.

7.4 Employees and workers should be mindful of the information they post on sites and make sure personal opinions are not published as being that of the Council. Misuse of such sites in a manner that is contrary to this and other policies could result in disciplinary action.

7.5 Employees and workers must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords which can make you vulnerable. In addition, employees and workers should:

- ensure that the correct privacy settings are set;
- ensure that no information is made available that could provide a person with unauthorised access to the Council and/or any confidential information.

7.6 If using social networks for investigations, e.g. recruitment, employee relations or debt recovery, all staff must seek advice from Corporate Enforcement or Legal Services. Failure to do so may constitute a breach of the Regulation of Investigatory Powers Act (RIPA). No covert social networking profiles must be set up or used.

7.7 Social networking should not be used for decision making. They are only to be used for ideas and ad-hoc communication. Decisions should only be communicated via formal methods of communication that allows for a formal recordletter to be created and kept such as email.

7.8 If using video conferencing sites all staff must conduct themselves in a professional manner ensuring

- You do not use the messaging function within web conferences to share personal or confidential information.
- Meetings are not recorded unless all participants have consented to be recorded and processes are in place for the secure storage, retention and destruction of the recording.
- If the web conference is with members of the public a password to access the meeting is set.
- You are aware of your surroundings, ensuring no confidential or personal information is seen, this could include members of the public in the background.

If the discussion is of a confidential or sensitive nature the conference must take place in a private area

8. Legal issues and points around the use of social networking and websites

8.1 Employees and workers should be familiar with the legal areas outlined below before writing about colleagues or sharing information about the Council. Examples of social networking activities outlawed under the Consumer Protection from Unfair Trading Regulations include:

- Creating fake blogs ('ghosting')
- Falsely representing oneself as a customer
- Falsely advertising on social networking sites
- Libel and defamation

8.2 Employees and workers must comply with the UK General Data Protection Regulation and Data Protection Act 2018. In particular, not sharing personal or confidential information inappropriately, checking location of information

if using new social networks and ensuring it is acceptable under the Data Protection legislation.

8.3 Information posted and responded to over social networking sites, including MS Teams and WhatsApp, that is deemed as official Council business may be subject to the Freedom of Information Act, Environmental Information Regulations and Data Protection Access Rights. Due to the complexity of officially recording and retrieving data posted on these sites all staff must ensure social networking sites are not used for official Council business and decision making.

8.4 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.

An organisation may be held responsible for something an employee has written or said if it is on behalf of the Council or on a Council-sanctioned space. The Council will take appropriate action in line with the disciplinary policy and procedure should a defamation incident occur. 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. Staff 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.

9. Reporting Procedures

9.1 As per the Council's Speak Up Policy and Data Security Breaches Policy, the Council encourages staff who suspect wrong-doing to report it, as it helps perpetuate the integrity of the Council, even if suspicion proves unfounded.

In the event you become aware of the misuse of social networking you should report this to your manager immediately. If reporting the incident to your manager is not possible please speak with Human Resources.

If an investigation into the misuse of social networking is required the Information Governance Manager may conduct the investigation.

Document revisions

Document revised (date)	Details of revisions made	Version
09/01/15	Updates	5
09/03/15	Updates	6
03/06/16	Updates	7
16/08/17	Updates	8
15/03/18	Updates	9
March 2021	Updates	10
April 2022	Updates and format	11