Renfrewshire Council

SOCIAL MEDIA GUIDANCE AND GUIDELINES

Social Media Policy and Guidance

1. Introduction

1.1 The Council recognises that social media has become part of everyday life for employees and can be used positively. All Council employees should be aware of their conduct and responsibilities when communicating online and using social media sites. This guidance provides information on the use of online communications and, in particular, social media and highlights examples of safer use. It also provides guidance on how unacceptable use may be addressed by the Council.

1.2 This guidance applies to all employees including temporary employees, casual workers and any volunteer, contractor or individual who has access to any Council social media accounts.

1.3 When engaged in online activities, including the use of social media, employees are reminded that the Council has a number of policies and procedures which clearly detail the standards of conduct and behaviour expected.

These include:

- The Code of Conduct for Employees
- Respect at Work Policy
- Disciplinary Policy
- ICT Acceptable Use Policy
- Surveillance Policy and Guidelines
- Data Protection Policy
- Information Security Policy
- Expressing Concerns outwith Line Management (Whistleblowing).

This guidance should be read in conjunction with these policies and associated professional codes of conduct.

2. What is social media?

2.1 Social media and social networking sites have become an extremely well-used and important communications channel. Social media includes software, applications (including those running on mobile devices), emails and websites that enables users to interact and create and exchange information online.

Examples include, but are not limited to:

- Blogs
- RSS feeds from other websites
- Social networking sites such as Facebook, Twitter, LinkedIn, SnapChat or What's App
- Photo sharing sites such as Flickr or Instagram
- Content sharing or bookmarking sites such as Digg and Delicious
- Customer feedback sites such as Yelp
- Video sharing sites such as YouTube
- SMS (text) and instant messaging programmes such as, MSN Messenger and BBM.

2.2 As the use and popularity of social media grows, the lines between what is public and private, personal and professional, overt and covert have blurred. While social media creates new opportunities for communication and collaboration, it also creates new responsibilities. Comments posted via social media can travel far and be difficult to remove. The purpose of this guidance, therefore, is to make clear the conduct and behaviours expected of employees of the Council who use online communication methods and, in particular, social media for business and personal use.

3. Employee responsibilities when at work

3.1 Employees who have their own personal profile on a social media website should be aware of their conduct and behaviour on these sites and their responsibilities to the Council. Posted material can, when matched with an identity or photograph, reflect not only on the individual, but also on that individual's employer, clients, colleagues and profession.

3.2 Social media can encourage casual and informal dialogue and very often innocent actions can easily be misconstrued or manipulated. Electronic messages are not anonymous and once information is online the author relinquishes control of it. Social media sites archive content posted, even when deleted from online profiles.

3.3 Employees are permitted to access social media sites such as Facebook and Twitter on the Council network for business purposes and for personal use outwith the employees' normal working hours, in accordance with the Council's ICT Acceptable Use Policy and these guidelines. Employees who are granted access to social media sites for work purposes should ensure they have read and fully understand the Council's Acceptable Use Policy and, where appropriate, abide by any professional code of conduct that applies to their role.

3.4 All employees are responsible for any information they make available online in a work or personal capacity whether this was posted during work hours, during breaks or when not at work. The Council will consider employees to be responsible and accountable for information contained on their social networking page or blog, even if that information originated from another source or was posted outwith normal working hours. They will also be held responsible and accountable for postings which have been copied by people entitled to access them and sent on to others beyond the control of the original poster.

3.5 This will apply where they are **identifiable as a Council employee** and the information or images posted are subsequently brought to the Council's attention. By **identifiable**, this means either through directly referring to themselves as a Council employee or indirectly identifying the Council as their employer through the information they post. Employees therefore must ensure that when engaging in social media activity they abide by the following standards:

Employees must not use social media sites to:

- Send or receive information or images online about the Council, its services, facilities, employees, customers or third parties, which may be considered confidential, offensive, defamatory, discriminatory, harassing, illegal, embarrassing, threatening, intimidating or which may incite hatred (e.g. sectarianism). The extent to which such information or images shall be regarded as meeting any of the above descriptions shall be judged in terms of the likelihood of the employee's comments causing harm or distress, the scale of any harm and the implications of such harm, whether physical, psychological, financial, reputational or commercial.
- Send or receive information and/or post comments or images online which may discredit or call the Council into disrepute. This can also include circumstances where comments, while not intended to be derogatory, may, if taken out of context, bring the Council into disrepute.
- participate or offer opinions online in regard to current or rumoured legal/commercial activities of the Council, for example, school closure

- send, receive or post images/photos of clients, service users or employees in the workplace without explicit consent
- discuss work-related issues and complaints in a manner which could cause distress to individuals, damage their own reputation or that of their employer. Any legitimate concerns should be addressed through the appropriate Council policies.
- use their Council email address to register on a social network unless they are setting up the account for business purposes.

When using social media for business purposes to communicate with service users, employees must:

- Get approval from their service
- get approval from the communications team prior to setting up any social media accounts
- identify a responsible social media owner
- undergo training to be approved social media account authors
- familiarise themselves with the 'Social Media and RIPSA fact sheet' *(see Appendix 1),* 'Social Media – Tips and Guidelines' *(see Appendix 2),* 'Social Media – Dos and Don'ts' *(see Appendix 3)*, 'Social Media – Checklist' *(see Appendix 4)* and our 'Social Media Guide for Business Users' *(contact the communications team or HR for a copy of this)*
- never use their Council email address to register on a social network unless they are setting up the account for business purposes.

3.6 Employees using social media for work purposes, particularly those with any form of enforcement or investigatory role must be aware of what covert surveillance is – this is **monitoring** someone who is **unaware** of they are being monitored to obtain **information**, usually for a specific investigation, even when this is easy to find or 'open source'.

3.7 Covert surveillance must usually be authorised by an Authorising Officer. Any employee who thinks that they could be using social media for covert surveillance must first check with his/her line manager or the authorising officer for his/her service. A list of authorising officers can be obtained from the managing solicitor, (Information Governance).
There is a difference between making use of publicly available information found on the internet or social media when making general observations and targeting a specific individual's social media pages, especially if this occurs more than once. It is important to understand the privacy settings of the social networking sites you are using to collect information, as not all social networking sites work in the same way.

3.8 Employees using social media for work purposes should not 'Friend' someone to get access to their activities or profile without them knowing who they are and what they are doing, before checking with their line manager or authorising officer. Employees must never set up a false identity for a covert purpose without first obtaining an authorisation.

3.9 Where employees bring their own personal mobile devices into the workplace, they must limit their use of these devices in relation to personal use of social media to official breaks, such as lunch breaks and outwith working hours. Working hours means the period of time that the individual spends at paid work (this is highlighted in the individual employee's contract of employment).

3.10 The expectation of an employee's behaviour when interacting with social media is no different from the expectation of their behaviour when dealing with other methods of communication, such as face-to-face or on the telephone. However, as with all other forms of communication, there may be circumstances where an employee's participation with social media is brought to the attention of the Council. Any incidents of unacceptable or inappropriate use of social media will be investigated by the Council and could result in disciplinary action, including dismissal.

3.11 If employees intend to post pictures or videos to Council accounts they must ensure that they or the photographer who took the images have obtained permission from the people in the photographs (children, service users, etc.) before posting them online.

4. Employee responsibilities when not at work

4.1 All employees are responsible for any information they make available online whether this is posted during work hours, breaks or when they are not at work. The Council considers employees to be responsible and accountable for information contained on their social networking page or blog. Employees need to be aware of what is posted/uploaded to sites they control and that they are expected to manage any inappropriate material responsibly and appropriately. If an employee comes into contact with any inappropriate material outwith their control, it is expected that this too is managed appropriately.

4.2 Employees who use their personal social media accounts to promote work events, initiatives and campaigns should include a line in their profiles stating the opinions expressed on the account are their own and do not reflect the Council's views (especially on Twitter).

5. Safer use of Social Media

5.1 Using online communication and social media can be a great way of keeping in touch with friends, family and work/professional colleagues.

To avoid any conflict between your personal use of social media and your employment with the Council, you should:

- Think twice before posting anything about the Council, your job or your colleagues
- Social media should not be used to, or appear to, promote, encourage or express any personal or political views/opinions which may bring the Council into disrepute, harm the Council's reputation or breach any of the Council's other policies. If in doubt, don't post it.
- ensure that profiles and related content are consistent with how you wish to present yourself to colleagues and professional contacts
- manage your privacy settings and keep them under review
- ensure your settings prohibit others from tagging you in any photos or updates without your permission and you can ask others to remove any undesirable content related to you
- regularly review your setting to ensure you know who has access to your information
- Be aware that conversations held online may not be private. Be aware of who may have access to what you post.
- do not use the Council's logo or branding materials in personal social networking accounts
- share information with care
- do not put comments online that are racist, sectarian, discriminatory, unlawful or unacceptable in any context
- comply with copyright and data protection laws, as libel, defamation and data protection laws still apply online.

5.2 Employees should speak to their manager if they believe they are being targeted online or believe that personal information may be used in a manner that might compromise their professional status.

6. Unacceptable use of Social Media

6.1 Examples of unacceptable and inappropriate online activity and use of social media are:

- Offensive or defamatory comments in relation to any employee, including management, colleagues or service users, of the Council, service user, customer or Elected Member

- posting of comments that may be considered as discriminatory, harassment, bullying or victimisation
- language or comments used in a discriminatory or defamatory way
- using photographs or video footage of an employee or service user of the Council without their permission
- Disclosure of personal, sensitive or confidential information gained during the course of your employment without authorisation. Unauthorised disclosure could constitute misconduct/gross-misconduct in accordance with the Council's Disciplinary Procedures.
- posting comments, content, media or information that could bring the Council into disrepute
- indecent, violent or offensive behaviour, while working on behalf of the Council, including the viewing, downloading and/or circulation of offensive or sexually explicit material
- harassment, bullying, discrimination, intimidation or victimisation against any individual(s) whilst working on behalf of the Council, or which can be connected to work by bringing the name of the Council into disrepute
- Behaviour during working hours and outwith working hours, which brings the name of the Council into disrepute.

6.2 Legitimate concerns about the Council or employees should be addressed through the appropriate HR policies and procedures, such as the Grievance Procedures or the Respect at Work Policy. Where through investigation it is found that use of social media has been unacceptable, this may lead to disciplinary action being taken and could lead to dismissal.

6.3 Inappropriate online behaviour, such as cyberbullying, can result in criminal action or in some instances civil action brought by others. Employees should also be aware that in circumstances where their behaviour is unlawful i.e., a hate crime incident such as sectarianism, racism or homophobia, the Council will report this to the Police.

7. Further information

7.1 Further information on this guidance can be obtained from your manager or HR and Organisational Development.

7.2 Additional guidance on covert surveillance can be obtained from the Council's Surveillance Policy and Guidelines and the attached Social Media Fact Sheet. Specific advice can be obtained from the Managing Solicitor (Information Governance).

Appendix 1: Social Media and RIPSA Fact Sheet

Do:

- Be aware of what covert surveillance is – this is **monitoring** someone who is **unaware** that they are being monitored to obtain **information**, usually for a specific investigation
- Know that using social media or the internet to obtain information about someone for a specific purpose, without their knowledge, even if this is part of your job, could be covert surveillance, even if this information is easy to find
- Remember that there are rules for use of covert surveillance, which involve applying for a RIPSA authorisation from an Authorising Officer in your service
- **Stop and check** with your Line Manager, before doing anything which you think could be covert surveillance
- Know the difference between making use of publicly available information you find on the internet or social media when making general observations and targeting a specific individual's social media pages, especially if more than once
- Understand the privacy settings of the social networking sites you are using to collect information, as not all social networking sites work in the same way

Don't:

- Assume that viewing "open source" materials for information about the person or his/her family will never need an authorisation because this is publicly available. Repeat viewing of this information may need to be authorised if this becomes targeted/focused.
- Bypass privacy settings to get information without the person's knowledge, without an authorisation
- 'Friend' someone to get access to their activities or profile without them knowing who you are and what you are doing, before checking with your Line Manager or Authorising Officer
- Ever set up a false identity for a covert purpose without first obtaining an authorisation
- Ever adopt the identity of someone known to users without his/her permission and without the Authorising Officer considering any harm to him/her

Appendix 2: Social Media – Tips and Guidelines

Top tips:

- Use a friendly tone and avoid 'Council speak'
- Encourage chat and discussion and don't be afraid to include questions in posts
- Listen to what people are saying
- Share good news/relevant information from partners/other positive local organisations
- Like positive comments and share positive posts about you
- Even routine information can be interesting. Tell people what you're doing!
- Use bitly (https://bitly.com) or Hootsuite (www.hootsuite.com) to shorten web links that you post/tweet
- For more information about how to improve your posts, read our house styles guides for Twitter and Facebook (contact the Communications team for this document)

Be clear who you are representing - Renfrewshire Council logo and information should be used on official council-affiliated social networking sites.

Manage expectations – if your site isn't going to be monitored 24/7 make this clear and provide alternative phone, email and website details in your profile/page information.

Make sure any posts you make are professional and uphold the council's reputation (see the attached 'Social Media – Policy and Guidance' on when to respond).

Remember that everything you post is a reflection of the council, always be clear in your language and never post anything that could be misconstrued or wrongly interpreted to reflect badly.

Don't endorse (or follow/like the pages of) political parties, candidates, or groups.

Be open. Private messages will be dealt with but private conversations shouldn't be encouraged.

Never share your personal information, e.g., name, job title, department or working situation, e.g. home working, to avoid exposing yourself or the council to risk.

Always double check facts, grammar and spelling, or have a colleague check, before posting.

Never use personal insults, obscenity or engage in any conduct that wouldn't be acceptable in the workplace or in a face-to-face meeting.

Don't post threatening, abusive, harassing, blackmailing or bullying messages (cyberbullying).

Don't endorse (or follow/like the pages of) any commercial products, services, or entities.

If you state in your personal social media profile that you work for the Council and/or you use your account to post about the Council/your team, include an 'All views expressed are my own' statement to your account profiles.

Appendix 3: Social Media – Dos and Don'ts

We use a number of social media platforms including Facebook, Twitter, Instagram and YouTube.

Most social media channels have their own rules and guidelines, which we always follow. We also have our own house rules to help you interact with us in a safe and appropriate way.

Dos and don'ts

Only post information you are happy for everyone to see.

Be civil, tasteful and relevant.

Don't swear or use offensive language.

Don't post anything unlawful, libellous, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented or racially offensive.

Don't incite, condone or encourage anything that could result in a criminal offence, civil liability or breaches any laws regarding competition.

Don't post inappropriate images or threatening, abusive, harassing, blackmailing and bullying messages online.

Don't post links or direct others to sites containing viruses, corrupted files or anything that could damage or interfere with computer hardware or software, or to material which is offensive, or may breach the terms of use of the relevant social media account.

Don't post content copied from elsewhere, which you don't own the copyright for.

Don't post the same message, or very similar messages, more than once, also called "spamming".

Don't publicise your, or anyone else's, personal information, such as contact details.

Don't advertise products or businesses.

Don't impersonate someone else.

Complaints

Social media should not be used for formal complaints. You can make a complaint online here (https://selfservice.renfrewshire.gov.uk/Ef3/General.jsp?form=SS_Comments&page=pg_customerdetails).

Endorsement

'Following' or 'Liking' another organisation or individual doesn't mean that the Council endorses them.

The views and opinions posted by others in our social media accounts are their own and not those of Renfrewshire Council.

While we try to ensure that the information on our sites is current, we can't guarantee that the information provided on our social media accounts will be complete, accurate or up-to-date.

This house rule information is available on the Council website and all Council affiliated social media accounts should include a link to it on their profile page (http://www.renfrewshire.gov.uk/socialmedia).

Appendix 4: Social Media Checklist

In hours:

- Check accounts and notifications first thing in the morning and throughout the day
- Check for mentions/posts to our page/direct messages
- Respond/acknowledge, e.g. provide answer if you can, signposting to webpages/phone numbers for more information, thanks for any positive comments (unless spam/trolls)
- Flag up any queries/issues/positive comments to relevant service
- Share, like, retweet or comment on any positive local stuff from our partners e.g. positive coverage of our news, information from community planning partners, local events or initiatives
- Check social media content plan/scheduled messages in Hootsuite to see what's coming up
- If there are gaps, schedule posts on useful information from our website e.g. how to report repairs online, check your bin collection, school holidays, etc. Run these posts past the relevant service before scheduling or posting.
- Flag up any emerging issues to the rest of the team/out-of-hours duty officer.

General:

- Everyone is responsible for posting their own news/campaign messages
- Social media slots will be left available in the content plan for news/campaigns each week. This information will be taken from the planner at the beginning of each week. Details of these slots will be emailed to the person in charge of the campaign/story at the beginning of the week after the social media content plan has been approved.
- If you need a social media slot ask for one. If this is not possible or it's out-of-hours, check the weekly social media content plan (I:\COMMUNICATIONS\02 JOB BAGS\05 2017\Digital\Social Media Content Plans\Weekly social media content plans) to see what spaces are available.
- Get your top line/key message in first few words
- Include links to more info on our website
- Every post should include an image, infographic or video
- For more information read our social media style guides (I:\COMMUNICATIONS\02 JOB BAGS\05 2017\Digital\Social media guidance and style guides)