COMHAIRLE NAN EILEAN SIAR

POLICY ON THE ACCEPTABLE USE OF SOCIAL MEDIA

2018

CONTENTS

1 INTRODUCTION

1.1 Social Media includes the various online technology tools that enable people to communicate easily via the internet to share information and resources. Social Media includes, but is not limited to, blogs, wikis, RSS feeds, social networking sites such as Facebook, Linkedin or MySpace, micro blogs such as Twitter; photosharing sites such as Flickr; and video sharing sites such as You Tube.

1.2 The use of social media can help support dialogue between the Comhairle, its partner agencies and the broader community. Such dialogue in the workplace can help all parties to engage with each other and supports the Comhairle's values of openness, fairness, flexibility and transparency.

1.3 The purpose of this Policy is to make clear what each individual's responsibilities are when using social media in a work capacity but also to highlight when these responsibilities cross into an individual's personal use of social media. Clear guidelines will be provided which will set the standard of good practice in the use of social media.

1.4 There are already a number of teams and departments who have their own social media channels, targeting difference audiences with different messages.

1.5 A list of all CNES social media accounts can be found on this web page.

2 BACKGROUND

2.1 Social Media has become an important communications channel. This technology, and the capabilities of the World Wide Web (www), often blurs the line between personal and professional communications.

2.2 Consequently, using social media creates additional responsibilities for employers and individuals, as material posted via social media (whether in a work or personal capacity), 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 SCOPE

3.1 This Policy, incorporating guidelines to different groups, applies to Members, Employees and Contractors.

4 LEGAL & POLICY FRAMEWORK

4.1 Photography & Video

a) Copyright

Users must have written permission from the original copyright-holder before using any photo or video. It is generally illegal to use imagery from the internet without permission,

Copyright cannot be transferred from a third party, Stock image libraries all have restrictions on usage. The licensing arrangements must be checked.

b) Images of Young or Vulnerable Persons

Images of young or vulnerable people must not be taken without written permission from their parent or guardian.

If a young or vulnerable person uploads a picture to a social media profile or page controlled by the Comhairle, the Comhairle could be held responsible for not acting upon it if it is later deemed to play a part in the offence.

c) Drone Photography

The Civil Aviation Authority has statutory guidelines for the use of a drone by an unlicensed operator:

- Do not fly within 50m of people or buildings
- Do not fly within 130m of, or over crowds or built-up areas
- Keep the drone in sight at all times
- Fly below 120m (400ft) if an aircraft is endangered, the operator could be jailed for up to five years

4.2 Personal Data

Any information relating to an identified or identifiable living individual is personal data. That will include photographs, video and audio recordings as well as writing. The presence of any personal data on social media will consitute "processing" of that data within the meaning of data protection legislation, and if it is on a medium for which the Comhairle is responsible, then the Comhairle has legal obligations as the controller of that data. Essentially, the Comhairle must respect the private nature of personal data and may only process it if it has a lawful reason for doing so. One lawful reason is that an individual has given their consent to the processing, but there are others which are more commonly applicable to public bodies. Employees must be satisfied that they have a legal right to use personal information before doing so. If they are unsure, they should seek advice from the Comhairle's Data Protection Officer.

4.3 The Comhairle supports managers and sets the standard for the use of social media through the implementation of its policies. The relevant policies are:

- Code of Conduct for Elected Members and Employees
- Information Security Policy
- Mobile and Landline Communications Policy
- Security Policy for Laptops and Portable Devices
- Equal Opportunities Policy
- Whistleblowing Policy, and
- Disciplinary Policy

4.4 All information posted using social media is subject to the Freedom of Information Act. As such the following principles, which form part of the Information Security Policy, must be adhered to:

- A named individual is responsible for keeping records,
- All information created as part of an employee's job role constitutes a Comhairle record, is evidence of the Comhairle's work and may be needed for reference by others in future,
- All information is subject to a retention period, specifying how long it must be kept.

5 USE OF SOCIAL MEDIA IN THE WORKPLACE

5.1 Social Media refers to websites and applications that enable users to create and share content or to participate in social networking. It is a key part of the Comhairle's communications strategy in relation to:

Communication – directly communicate important and timely messages, news and information, promote events and improve awareness of the service

Engagement – seek opinions and engage with the community to improve knowledge

Collaboration – find better and more effective ways of working with the community

Advertising – promotion of a range of services to various audiences.

5.2 Persons who wish to use an existing social media profile or page should contact the Communications Team, Chief Executive's Department. New social media channels must be approved by the Communications Team. The Communications Team will respond when the completed Social Media brief is received.

5.3 The Communications Team will ensure that ownership of all accounts is centralised and that only appropriate users have access. This manages the risk for the Comhairle and ensures the central record of existing accounts and activity is maintained.

5.4 For a new profile or page to be approved there must be evidence of user need for it and the resources identified to maintain it. Failure to maintain social media channels may result in the profile or page being deleted.

6 USING SOCIAL MEDIA FOR BUSINESS USE

6.1 When employees are using social media in the workplace they have a responsibility to use this in an appropriate manner. The following points should help guide employees and additional guidance on social media content and etiquette is attached at Appendix C:

- **You should not use any social media tool for Comhairle business unless you have received appropriate training.** You must apply for and be registered on the approved business social media user list held by the Chief Executive;

- If having read this document you are still uncertain about the appropriateness of publishing something online, it is best to **hold back and seek the advice** of your line manager and the Communications Officer. Also bear in mind the Comhairle's Information Management Guidelines.

- Many people post online working anonymously, using pseudonyms. The Comhairle discourages this in all forms of online participation that relate to the Comhairle. We believe in transparency and honesty. If you are posting about your work for the Comhairle, we encourage you to **identify yourself, be clear who you are, and identify that you work for the Comhairle.** If you have a vested interest in something you are talking about, ensure you have made this clear. What you publish will be around for a long time so consider the content carefully and also be sensible about disclosing personal details.

- **Follow copyright and data protection laws.** For the Comhairle's protection as well as your own, it is critical that you stay within the legal framework and be aware that libel, defamation, copyright and data protection laws apply. Ask permission to publish or report on conversations that you take part in at work. Be aware that content on social media websites may be subject to Freedom of Information requests.

- Remember that if you **break the law** using social media (for example by posting something defamatory), you will be personally responsible. You may also be subject to the Comhairle's Disciplinary Procedure.

- The Comhairle's reputation is made up in a large part by the behaviour of its employees, and everything you publish reflects on how Comhairle nan Eilean Siar is perceived. Social media should be used in a way that **adds value** to the Comhairle's business. If it helps you, your colleagues, our citizens or our partners to do your jobs and solve problems; if it enhances the

Comhairle's services, processes and policies; if it creates a sense of community; or if it helps to promote the Comhairle's aims and values, then it is adding value.

- Though not directly Comhairle-related, background information you **choose to share** about yourself, such as information about your family or personal interests, may be useful in helping establish a relationship between you and your readers, but it is your decision to share this information. You should be aware that by revealing certain details you might be more vulnerable to identity theft.

- **Don't be defensive.** When you see inaccuracies articulated about the Comhairle by citizens, journalists or by other bloggers, you may use social media channels - or join someone else's - to politely and sensitively point out the situation as you see it. You must also let your communications adviser know that you have identified information that is inaccurate or could damage the reputation of the organisation.

- **Be prepared for a two-way conversation.** And be aware that people are entitled to their views. You must make sure that what you say is factual and avoid becoming involved in unnecessary or unproductive arguments.

- If a conversation turns and becomes offensive in terms of language or sentiment, handle this **swiftly and with sensitivity**, remove the comment(s), and make sure you inform your audience exactly why you have done this. A few sentences should suffice, along the lines of: **"**This comment was removed because the content was offensive. Comments are welcomed but please respect the views of everybody who comes here."

- If you make a mistake, **be up front about your error and correct it quickly**. If you choose to modify an earlier post, make it clear that you have done so. Remember that there are consequences to what you publish. If you're about to publish something that makes you uncomfortable, review the suggestions in this document. If you're still uncertain, discuss it with your manager or with the Communications team.

- Be mindful that social media sites can be used to distribute malware, i.e. viruses. Employees should be aware that downloading applications or accessing links, for example the use of shortened urls in Twitter, can fool users into accessing unsuitable or malicious sites. So **take care with shortened urls**, unless you are following as organization or individual you can trust.

7 USING SOCIAL MEDIA FOR PERSONAL USE

7.1 As the use and popularity of social media grows, the lines between what is public and private, personal and professional have blurred. The Comhairle respects their employee's right to personal use of social media out-with the workplace.

7.2 However, each employee should be aware that actions in and outside work that affect the individual's work performance, the work of others, or adversely affect the Comhairle's reputation, may become a matter for the Comhairle.

7.3 Considering the following points may help avoid any conflict between your personal use of social media and employment with the Comhairle:

- If you already use social networks or blogs for personal use and you have indicated in any way that you work for Comhairle nan Eilean Siar you should **remove these.** The personal image you project in social media affects your **reputation** and may affect the reputation of Comhairle nan Eilean Siar. Sounding off about the Comhairle, even on a personal blog can be damaging. By identifying yourself as a Comhairle employee within a social network, you are connecting to your colleagues, managers and even Comhairle citizens.
- When using social media for personal purposes, you must not imply you are speaking for the Comhairle. Avoid use of the Comhairle e-mail address, Comhairle logos or other Comhairle identification. Make it clear that what you say is representative of your views and opinions and not necessarily the views and opinions of the Comhairle.
- You must comply with other **Comhairle policies** when using social media. For example, you should be careful not to breach Comhairle confidentiality and information security or information management policies, or the Comhairle's Code of Conduct. If in doubt, don't post it.

- Don't make the mistake of thinking that everyone linked to your page is actually your "friend", **don't include sensitive personal details** like your employer or your address. Your real friends already know, and you should choose carefully who else you give that information to.
- Be mindful of your **privacy settings**, if you want the world to see what you are doing and saying, be aware that you could be held accountable for it.
- Remember if you **associate yourself** with another Facebook user or site you could be linked with postings and contents on that page.
- Racism, sectarianism or other types of discrimination are **unlawful and are not acceptable** in any context. Putting these comments on line effectively puts them in print.
- **Follow** copyright and data protection laws, as libel, defamation and data protection; laws apply to you.
- Use your **common sense**, social media is a great way of keeping in touch with friends and family, just be sure you enjoy it sensibly.

8 NON-COMPLIANCE WITH SOCIAL MEDIA POLICY AND GUIDELINES

8.1 Expectations of employee's behaviour when interacting with social media are no different from expectation of their behaviour when dealing with other methods of communication, such as face-to face or on the telephone.

8.2 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 Comhairle. An example of this may be on receipt of a formal complaint or via some form of publicity. In these circumstances, and dependant on the nature of the complaint this may require further investigation, and may be subject to the Comhairle's Disciplinary Procedure.

8.3 Some examples of where this may occur are detailed below:

- Abuse or breach of any Comhairle nan Eilean Siar Policy or rule by which employees are bound to comply with.
- Serious misuse or abuse of Comhairle computer systems and non-compliance of security policies.
- Being charged with a serious criminal offence and/or an offence involving dishonesty, which, in the view of the Comhairle, affects the employee's suitability for continued employment.
- Indecent, violent or offensive behaviour, while working on behalf of the Comhairle, 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 Comhairle, or which can be connected to work by bringing the name of the Comhairle into disrepute.
- Behaviour during working hours and in some cases out-with working hours, which brings the name of the Comhairle into disrepute.
- Inappropriate disclosures of confidential information. For example information disclosed without the express consent of an individual, or disclosure of Comhairle nan Eilean Siar information to external organisations, which breaches Comhairle policy or legislation, unless covered by "The Public Interest Disclosure Act" or any other Act.

8.4 Employees should also be aware that where there is a serious breach of the Comhairle's Social Media Policy, that the Comhairle may be obligated to report these to the Police, for example making racial or sectarian comments.

8.5 Employees should also be aware that where they have a complaints or a grievance against either a colleague or the Comhairle, that there are formal procedures in place for progressing these.

9 SECURITY

9.1 As previously stated staff should not include comments on work on social media personal accounts. Police Scotland guidance on cyber threats include social media, Linkedin and online presence of staff as vulnerabilities. The recommendations for for cyber-resilience that social media users be vigilant about the information they post. Employees can be targeted using data on social networks which can result in a hoax email being sent to carry out an attack or introduce malware into the system.

10 RISKS

10.1 The table below details the risks and control factors relating to social media:

Risk
Criticism from the public/community (quality of information, timing, administration of media account, etc)

Control
A business case must be established for using social media and there must be an evaluation of its impact. The Communication Team will monitor and take action of standard is not reached. Social media users will have to be contacted and made aware of need for an annual(?) evaluation by the IT/Communications Team.

Risk
Technical security of accounts and potential for hacking.

Control
. Don't think this is possible. Only page admins have access to passwords and must take responsibility for the security of their page in line with the social media guidelines. Account details and passwords will not be shared with unauthorised users. All social media pages must have at least two authorised users and contact e-mail addresses must be given to the IT/Communications Team.

Risk
Unsuitable content from other users.

Control
Unsuitable posts and comments will be removed as soon as possible by the Communication/IT Team. This isn't possible due to page access restrictions. The Communication/IT Team will have a database of contact e-mail addresses for all page admins and can at any time instruct the immediate removal of posts, comments or, in extreme circumstances, the deletion of a page.

Risk
Damage to the Comhairle's reputation.

Control
All social media may be monitored and damaging content will be referred to the appropriate Director. Major problems will be reported to Corporate Management Team (CMT).

Risk
Inappropriate use by employees.

Control
All users of Social Media must adhere to the Policy. Failure to do so may be considered through the Disciplinary Procedure. Training and support will be made available from the Communication Team.

11 FURTHER INFORMATION

11.1 A number of professional bodies have issued guidelines to instruct their Members. The Scottish Social Services Council have published guidelines on their website titled 'Social Media Guidance for Social Services Workers'.

11.2 Code 5.8 of the Code of Practice for Social Services Workers says:

"I will not behave, while in or outside work, in a way which would bring my suitability to work in Social Services into question."

This statement includes using social media and extending to online behaviour. Employees who are registered with the SSSC must be aware of their published guidelines in addition to employee's responsibilities in relation to this Policy.

11.3 Elected Members have reference to conduct, extending to social media, as part of the Code of Conduct for Elected Members, Guidelines for Elected Members is attached at Appendix 1.

12 REVIEW

This Policy will be updated in line with best practice and legislative requirement and will be subject to review in three years.

APPENDIX 1

GUIDANCE TO ELECTED MEMBERS ON THE ACCEPTABLE USE OF SOCIAL MEDIA

1 BACKGROUND

1.1 The use of social media has changed the way that Elected Members can communicate whilst undertaking their duties. Social media can increase accessibility of Elected Members and offer new ways in which to engage with constituents, stakeholders and the general public.

1.2 The principles contained within the general policy on the use of social media should be adhered to when Elected Members set up social media accounts and communicate with the community.

1.3 Members are reminded of their responsibility for ensuring they comply with all relevant legislation when using social media, including the Councillors Code of Conduct, and the need to be considerate and courteous to fellow councillors and members of staff when using social media.

2 USE OF SOCIAL MEDIA DURING COUNCIL MEETINGS

2.1 Elected Members are free to use social networking from mobile devices at any time outwith meetings as a means of communication with the public, colleagues and officers. The unrestricted access recognises the need for elected members to engage with their communities via this means of communication.

2.2 The Comhairle will allow the use of hand-held electronic devices in formal council and committee meetings (including accessing social media and the internet), provided that they are silent, and used in a way that does not impair decorum; and that Members making speeches in the council or in committee may refer to electronic devices in place of paper speaking notes.

2.3 Elected Members will follow the following guidance:

- **Use of Mobile Devices:** Elected Members may use mobile devices (such as a laptop, ipad, tablet) to follow agenda items in committee papers or deliver pre-prepared speeches during public debate.

- **Regulatory meetings (planning and licensing) and private discussions/briefings at Council/Committee meetings:** In keeping with the spirit of the Councillors' Code of Conduct governing regulatory committee meetings, mobile devices, including mobile phones, should not be used for any form of communication (text or tweet) during business. This measure is to avoid any communication from a member of the public with an elected member which could influence the outcome of an application under discussion. 7.4 of the Councillors' Code of Conduct governing fairness and impartiality, states: "To reduce the risk of your, or your Council's, decisions being legally challenged, you must not only avoid impropriety, but must at all times avoid any occasion for suspicion and any appearance of improper conduct."

- This restriction also applies to discussions at full Council or Committee meetings held in private or confidential briefings.

- **Photographs:** Without the explicit consent of the Chair, photographs should not be taken or transmitted during a Council meeting.

- **Mobile Phones:** At all times during meetings, mobile phones should remain on silent or be switched off.