Social Media Protocol for Members

1. Introduction

1.1 Social media is one of the most important, and growing, means of communication for individuals and organisations. The Authority wishes to support Members' use of new technology, including social media. This Protocol is intended to provide guidance to help Members use social media in a way that avoids legal and reputational risk. It complements the general rules under the Code of Conduct for Members. As Members might expect, the basic position is that the same standards of behaviour and conduct apply online as would be expected offline. Some do's and don'ts when using social media are attached as **Appendix 1** to this Protocol. The principles of this Protocol are equally applicable to the use of e-mail communication by Members.

2. What are Social Media?

2.1 Social media is the term to describe websites and applications that enable users to create and share content or to participate in social networking. The content could comprise images, video, text, polls and links to web content.

2.2 On social media sites users share information, discuss opinions and may create interest groups or pages. Ultimately people use these sites and tools to build online communities and networks which encourage participation and engagement.

2.3 It is not a requirement for Members to have a Facebook, X (formerly known as Twitter) or Instagram account or use other forms of social media. However, if you are already using or planning to use social media in connection with your work as a Member of the Authority, or are already using such media in your private capacity, these guidelines will be relevant.

2.4 Social Media can be used:

- To support Members in performing their community leadership role by effectively engaging and interacting with residents
- To keep in touch with local views and opinions
- For campaigning on local and national issues of relevance to National Park Authorities

3. Types of Social Media

3.1 There are different types of social media:

- **Social Networking -** For example, Facebook, X (formerly known as Twitter) , Threads, WhatsApp and, LinkedIn. These applications allow users to post, share and respond to each other's content, directly connect with others as friends or fans and to form communities and discuss relevant news within those communities [1].
- **Photo Sharing -** For example, Instagram, Snapchat, Flickr and Pinterest. These sites allow users to post images and short videos alongside a caption. On sites like Instagram this can also include live video as Instagram Stories which disappear after 24hrs or Reels Instagram has features to enhance video production from mobile phones.
- **Video Sharing -** For example, YouTube and Vimeo. These sites allow users to share and interact with longer form video content.
- **Interactive Media** (mostly video) **-** For example, Snapchat and TikTok. These Apps allow users to share photos and videos. They also have a variety of unique interactive features including augmented and virtual reality filters, musical overlays, and games.

4. Things to consider

4.1 Any form of communication is capable of being misunderstood. While the use of social media should not in theory be more susceptible to this problem than any other form of communication, something about the immediacy of social media seems to magnify the problem. In addition, it is now almost impossible to delete published social posts in order to stop it being shared.

4.2 By the nature of such media, "misfiring", or being misunderstood, particularly with regard to something that is perceived as being more controversial than it was intended to be, is likely to lead to rapid and wide broadcasting of that apparently "controversial", misunderstood item.

4.3 There are no special, additional legal or ethical burdens relating to the use of social media. The same rules apply that govern the rest of your behaviour as a Member of the Authority, you just need to consider them in this context.

4.4 Although the best use of social media is conversational in tone, publishing online is still publishing. What you have said online is written down and it is permanent. Most pitfalls will be avoided if your online content is accurate, informative, balanced and objective.

4.5 Members should be careful to avoid saying anything that they wouldn't be comfortable repeating or justifying, for example, at a public meeting.

5. Legal issues

5.1 Libel – If you publish an untrue statement about a person which is damaging to their reputation, they may take a libel action against you. The same thing may happen if someone else publishes something libellous on your social media account, you know about it and don't take swift action to remove it. A successful libel claim could result in the award of damages against you.

5.2 Copyright – Placing images, text or music on your site from a copyrighted source (for example, extracts from publications or photos,) without obtaining permission, is likely to breach copyright laws. Therefore do not publish anything you are unsure about, or obtain prior permission. Again, a successful claim for breach of copyright would be likely to lead to an award of damages against you.

5.3 Data Protection – Do not publish the personal data of individuals unless you have their express permission.

5.4 Bias and Predetermination – If you are involved in making planning decisions, do not say anything through social media (or indeed anywhere) that suggests you have made your mind up on an issue that is due to be formally decided upon. While your likely view on a particular application may be well known, you need to be able to show that you attended the relevant committee meeting prepared to take on board and weigh all the evidence and arguments, and were genuinely persuadable to a different view. Otherwise the decision may be later challenged as invalid. If a person has suffered some sort of detriment as a result of such an invalid decision, they may have a claim against the Authority for damages.

5.5 The Cabinet Officer has banned the use of the TikTok application on any Government owned electronic device following a security review which looked at the potential vulnerability of government data from social media apps on devices and risks around how sensitive information could be accessed and used by some platforms.

6. Social Media and the Code of Conduct for Members:

6.1 Aspects of the Code of Conduct for Members will apply to your online activity in the same way as they do to any other written or verbal communication you may engage in. The key to whether your online activity is subject to the Code is whether you are, or appear to be, acting in your capacity as a Member rather than as a private individual.

7. Particularly relevant elements of the Members' Code of Conduct

7.1 You must treat others with courtesy and respect - do not use social media to make personal attacks or indulge in disrespectful or offensive comments.

7.2 You must not intimidate or attempt to intimidate any person – do not say anything, particularly if it is part of a series of similar comments about a person or on a theme that might be construed as intimidation, whether the comments relate to an Authority employee, a fellow Member or anyone else.

7.3 You must not bring the Authority into disrepute – you should not publish anything that could reasonably be perceived as bringing yourself as a Member, or the Authority in general, into disrepute.

7.4 You must not disclose confidential information, through your use of social media, just as in any other circumstances, you would not disclose information given to you in confidence by anyone, or information acquired by you which you believe, or ought reasonably to be aware, is of a confidential nature.

7.5 Inadvertent leaks of the Authority's confidential information are more likely to take place when a Member is using social media, rather than when they are carefully drafting a letter for publication in the local paper. This may be because of the more immediate, conversational, off- the cuff nature of much social media communication. Members must be careful to apply exactly the same Code of Conduct standards to their social media communications as they would to statements made in a more formal context.

8. Further advice

8.1 The Monitoring Officer and the Communications Team are happy to help Members by providing additional advice and guidance as appropriate. Training is also available to individual Members on the use of social media.

8.2 Reference can also be made to the National Park Authority's Social Media Strategy and the wider Social Media Guidelines.

9. Responsibility for the Protocol

9.1 The Monitoring Officer has overall responsibility for this Protocol and will review its operation in accordance with the Authority's policy review timetable or sooner where appropriate.

December 2023

Appendix 1

Do's and Don'ts when using Social Media

Do:

- be responsible and respectful at all times.
- set appropriate privacy settings for your social media channels.
- keep an eye out for defamatory or obscene posts from others on your social media and remove them as soon as possible to avoid the perception that you condone such views.
- be aware that the higher your profile as a Member, the more likely it is you will be seen as acting in your official capacity when you post on social media.
- ensure you use Authority facilities appropriately; if you contribute to an Authority blog or social media post, any comments you make will be viewed as being made in your official capacity.
- be aware that you will be seen as acting in your official capacity if you publish information that you could only have accessed or be perceived to only have accessed by being a Member of the Authority.
- feel able to make political points but be careful about being too specific or personal if referring to individuals. An attack on an individual may be seen as disrespectful, whereas general comments about another party or genuine comments on policy are less likely to be viewed as disrespectful.

Don't:

- Post in haste, particularly in circumstances where your judgement might be impaired.
- make unguarded statements which could lead to potential liability.
- post comments that you would not be prepared to make on paper or face to face.
- use Authority facilities for personal or political posts.
- request or accept a contractor providing services to the Authority as a "friend" on a social networking site where this suggests close personal association. For the avoidance of doubt, this does not apply to sites which are intended as a neutral, professional connections registry (such as Linkedin).
- use social media in any way to attack, insult, abuse, defame or otherwise make negative, offensive or discriminatory comments about members of the public, Authority staff, their family or friends, colleagues, other professionals, other organisations, or the Authority.

- publish confidential information that you may have learned or had access to as part of your role as member of the Authority. This includes personal information about contractors, Authority officers as well as Authority related information.
- represent your personal views, or those of any political party or interest group you belong to, as being those of the Authority, on any social medium.
- browse, download, upload or distribute any material that could be considered defamatory, illegal or discriminatory.
- make conspicuous, excessive and continuous use of social media technology during the course of an Authority meeting or committee meeting so that you give the impression to the public of not being respectful of the proceedings and, more seriously, taking decisions that are not based on full engagement with the facts and arguments.

This Protocol was approved by the Standards Committee on 5 December 2023 and adopted by the Authority on 12 December 2023. It is due for review in December 2028.