Policy on using social media

January 2021

Contents

Purpose and scope

This policy guides the Broads Authority on the appropriate use of social media. The policy applies to:

- The professional use of social media on behalf of the Authority by its Communications Team
- The use of social media by Authority members (including co-opted members) and officers when referencing, or when identified as being affiliated with, the Authority; and
- The use of social media by consultants, interns, agency workers and casual workers engaged by the Authority when referencing the Authority.

When using social media to refer to or comment on the Authority's work, processes, or members or officers, you may well be acting in your capacity as an officer or member of the Authority, and if found to be so, this policy will apply to such use.

All members and officers must make sure they comply with this policy, which should be read with the following Authority documents, as relevant:

- Code of Conduct for Members
- Code of Conduct for Employees

- Protocol on Member and Officer Relations

Definition of social media

For the purposes of this policy, 'social media' means any type of online media that allows users to create and share content with others online, and to participate in social networking, discussion and interaction. This includes, but is not limited to:

- Social networking, such as Facebook, LinkedIn, Google+ or Yammer
- Microblogging, such as Twitter or Tumblr
- Photo sharing, such as Instagram, Snapchat, Pinterest or Flickr
- Video sharing, such as YouTube, Facebook Live, Periscope or Vimeo

This policy also covers private messaging through online channels such as Facebook, Twitter and WhatsApp.

Members or officers with any questions about the general use of social media should contact the Communications Team for advice.

Broads Authority accounts

The Broads Authority has the following corporate social media accounts:

- Facebook: https://www.facebook.com/BroadsAuthority/
- Twitter: https://twitter.com/BroadsAuth
- Instagram: #broadsauthority
- Linkedin: Broads Authority

It also manages social media accounts on various platforms for the Broads National Park.

These accounts are managed and administered by the Communications Team and should be used for most Authority-related social media activity. Other corporate accounts should not be set up without prior consultation with the Communications Team.

Within a business context, carefully managed social media is essential in:

- Publicising and promoting activities that enhance the Authority's reputation, its services and the partners and communities it works with;
- Promoting and strengthening the Authority's brand;
- Responding to questions from the public, businesses and other interests;
- Clarifying or correcting unclear or misleading views or statements;
- Giving information and guidance, including advice in emergency situations;

- Engaging with the public about the services the Authority provides, and promoting their understanding and enjoyment of the Broads.

It takes a lot of time and effort to manage a social media account effectively and build up a good network of followers. It is important to maintain a consistent and professional approach across the Authority's social media channels.

The Communications Team will work with Authority colleagues to encourage good use of social media, and can provide guidance and training.

Rules for Broads Authority accounts

Individual officers should not be named in Authority social media posts. This is to avoid compromising personal social media accounts with inappropriate followers or 'trolls' (people who post inflammatory, offensive or off-topic messages online).

All information and comments posted by the Authority will be seen as being associated with the organisation and will count as public statements on record. As such, they may be used as a reference at any time in the future.

The Communications Team will not post or disclose on social media:

- any politically sensitive or controversial information, or matters that could reasonably be considered as such; or
- confidential information gained by officers or members as part of their role, including personal information about people and confidential information relating to the Authority. This requirement will continue after the officer or member leave the Authority's employment or ceases to be a member.

Personal accounts

The following guidelines apply to all Authority officers, and to members whose personal social media accounts identify them as a member or co-opted member of the Authority.

If you use social media for personal use, and have indicated that you are an Authority member or officer, you should consider using a disclaimer that states that the opinions on your personal site are your own – for example, "The views expressed on this site are my own and do not reflect the views of the Broads Authority" (or "the views of my employer", as applicable).

Some members are also members of another authority or body, and their profile will indicate this. If this applies to you, you should make clear in what capacity you are expressing any views. Remember, even if you do not expressly state on social media that you are a member of the Authority, this policy will apply if a connection with the Authority can reasonably be made.

When posting content on social media, always be mindful of the impact your comments may have on the Authority's reputation, and on its members and officers. You are

personally responsible for the content you publish. What you publish may be around for a long time, so consider it carefully before publishing it.

Never disclose commercially sensitive, anti-competitive, private or confidential information, and be sensible about disclosing personal details.

Social media networks, blogs and other types of online content are monitored by journalists to generate press and media content or legal questions. You should refer such enquiries to the Head of Communications. The Communications Team will monitor social media and respond where appropriate to inaccuracies or comments that could damage the Authority's reputation.

You must make sure you comply with data protection legislation in your posts. For example, you may need to move a public discussion to private messaging (Facebook) or Direct Message (Twitter) when discussing personal details, or ask someone to contact you in a private way, such as by telephone or email.

The Authority will not tolerate any of the following activity on social media, if it can be connected to you as a member or officer of the Authority:

- Abusive or threatening behaviour;
- Posting inappropriate comments or material that could be regarded as discriminatory;
- Misleading or false statements that could adversely affect the Authority's reputation;
- Inciting or supporting the commission of crime or unlawful acts; or
- Sharing or liking any of the activities referenced in this paragraph, as this could suggest that you approve of such activities.

If you feel you have been subject to cyber-bullying, or feel offended by material posted or uploaded through any digital communication network, officers should inform their line manager and members should inform the Monitoring Officer. For your own protection, you may 'block', 'hide' or 'ban' abusive users.

You must consider carefully who you accept through a 'friend request'. Accept a request only if you are sure it will not put you, as a member or officer, in the position of having a real or apparent conflict of interest.

If your online activities through social media are considered to be in breach of this policy, the Authority may require you to remove content that, in its reasonable opinion, breaches this policy.

Social media and the Code of Conduct for Members

S27(1) of the Localism Act 2011 say that a relevant authority must promote and maintain high standards of conduct by members and co-opted members of the authority. S27(2) of the Act says that in discharging its duty under subsection (1) a relevant authority must, in

particular, adopt a code dealing with the conduct that is expected of members and co-opted members of the authority when they are “acting in that capacity.”

If there is a complaint made against a member under the Authority’s Code of Conduct (the Code) about their use of social media, it must first be decided if the post was made by the member while acting in their official role, or in their private capacity. This decision is fact specific, and will depend on the exact circumstances of each case. That is why it is not easy to give clear examples of what may, or may not be, “in capacity”.

However, it is recommended that members are clear in their communications about whether they are posting/tweeting, etc in their official role or in a private capacity. If you are acting in your role as an Authority member when using social media, and posting accordingly, the Code will apply to you. The Code may also apply if you are using your personal social media to comment on the Authority’s business, members or officers. While the Code is not there to police your freedom of expression or your personal social media accounts, it may be wise to take special care if you use a private account to comment on or disclose the Authority’s business, make personal comments about other members or officers, or write about things that you know only through being a member. An image of your comment could be copied to a public group, for example.

Members should also bear in mind that if communications are made public, even if they are sent in a private capacity, the media and the wider general public may not make the distinction between what is in capacity, and what is not. Please also note the point about the use of disclaimers when using personal social media accounts, as explained above.

Legal issues

The use of social media can bring the same legal issues as the use of any other media. The key difference is that, with social media, breaches of the law can become apparent very quickly and to a potentially huge audience.

You should be familiar with legal risks, including:

- Breach of copyright by using a third-party image or written material without permission: Make sure you have permission to use any photographs, film, sound recordings or printed material that is not your own.
- Defamation: Writing something about an individual or body that is considered to harm reputation can, and does, lead to significant claims for damages in the courts.
- Breach of the Malicious Communications Act 1988 or section 127 of the Communications Act 2003: This includes sending messages designed to cause anxiety or distress, or of an offensive or menacing character. These are criminal offences.
- Unfair Trading Regulations: These prohibit fake blogs, falsely representing oneself as a customer and falsely advertising on social media sites.

- Making comments that suggest you are predetermined or biased in relation to a planning issue.
- Safeguarding: Do not take or use any photographs of children who appear to be under the age of 18 years without permission from a parent or guardian.
- Cyber-bullying: Although there is no legal definition of cyber-bullying in UK law, a number of existing laws can be applied to cyber-bullying and online harassment that could constitute a criminal offence. Never upload, post, link to or forward any abusive, obscene, discriminatory, harassing, derogatory or defamatory content. This includes posts about your colleagues, members of the public or the Broads Authority as an organisation.

Any such breaches could result in disciplinary or Code of Conduct action.

What happens if you make a mistake?

If you are aware that you have posted something inappropriate in relation to the Authority on a personal social media channel, it is important to be open and honest about your mistake, while also being quick to correct it.

Officers should tell their line manager immediately and consult with them and the Head of Communications to agree action to avoid or minimise embarrassment or reputational damage to the Authority. Members should contact the Head of Communications for advice.

Contacts

This version of the policy was adopted by the Broads Authority in January 2021. It will be reviewed regularly and may be withdrawn, amended, suspended or departed from at any time at the Authority's discretion.

For information or advice, please contact:

Rob Leigh, Head of Communications
Broads Authority, Yare House, 62-64 Thorpe Road, Norwich NR1 1RY
Email: Rob.leigh@broads-authority.gov.uk
Tel: 01603 756049

Monitoring Officer
Broads Authority, Yare House, 62-64 Thorpe Road, Norwich NR1 1RY
Email: monitoring.officer@broads-authority.gov.uk