



Social Media Policy

April 2020



Table of Contents

1.	Introduction.....	3
2.	Who can use our corporate social media accounts?	3
3.	How to use our corporate social media accounts.....	4
4.	Security.....	8
5.	Personal use of social media	9
6.	Use of social media by councillors	11
7.	Further information	12

1. Introduction

Social media plays a huge role in the work of Buckinghamshire Council and in the lives of many employees and customers. As a local government organisation, we can use social media channels to communicate our key messages, share relevant news, and respond to queries from our audiences.

However, social media also comes with some safety, confidentiality and reputational risks, both to our staff and to the organisation as a whole.

This policy is intended to get the most out of social media for Buckinghamshire Council while protecting our staff and our reputation, and minimising any risk. The policy should be viewed alongside the staff [Code of Conduct](#).

The majority of this document applies to Buckinghamshire Council officers but there is also a section for members, which should be read alongside the members' [Code of Conduct](#).

What is social media?

The term 'social media' refers to websites and applications that allow users to create a profile and share information, ideas and news through virtual communities (social networks).

This content most often comes in the form of text posts, photos, videos, or comments on other people's posts. Popular sites include Facebook, Twitter, Instagram, LinkedIn and YouTube.

2. Who can use our corporate social media accounts?

All staff required to use social media on behalf of Buckinghamshire Council will be offered training by the Communications team. Managers should ensure that training is provided for all staff who are required to use social media as part of their job role.

Where ownership and accountability lies

- The Communications Team is responsible for managing, publishing and monitoring content on the corporate Buckinghamshire Council social media accounts.
- Buckinghamshire Council will only post on our own social media accounts so that we are able to monitor any incoming comments and provide information and guidance where necessary. We do not respond to criticism or negative comments on community channels due to the resource implications.
- Where we want to share key messages or community events on third party or local community channels, it's preferable to ask the manager of that channel to do so. Failing this, an officer or councillor may create the post on the Council's behalf.
- Staff who use social media as part of their job must adhere to the staff [Code of Conduct](#), as they would in any work they carry out. Employees should be aware that they are representing Buckinghamshire Council and are personally responsible for any social media content they publish.

Are there any exceptions?

- To ensure consistency in our responses, access to Buckinghamshire Council social media accounts is primarily limited to the Communications Team.
- In circumstances where there is a sound business case for a project or team having a separate account, the Communications Team will consider a request for a new account. Please contact the Communications Team for the account request form.
- Before an account or page is requested, the level of engagement needed, the resources required and the timeframe all need to be agreed with the relevant senior manager.

3. How to use our corporate social media accounts

Buckinghamshire Council uses the following social media platforms: Facebook, Instagram, LinkedIn, Twitter, YouTube. All of these accounts – and any future accounts representing the Council – must be used in line with this policy and the staff [Code of Conduct](#).

General

- Before uploading Buckinghamshire Council material onto a social networking site, you should make sure that you are aware of, and comfortable with, the site's own terms and conditions.
- Staff should be sensitive to the minimum age requirements on different social networking sites (this is often set at age 13).
- Keep your communications clear, positive, polite and professional.
- Make sure that any information you are posting, commenting on or sharing is accurate, reliable, not prejudiced and not 'fake news'.
- Content must never bring the Council into disrepute, for example by criticising, disagreeing or arguing with customers, colleagues or managers; making defamatory remarks about individuals or groups; posting inappropriate images or links.
- It's important that content is not open to misinterpretation. Once published, content is almost impossible to control and may be manipulated, used in different contexts and further distributed, potentially damaging our brand and reputation.
- If content is misunderstood, then clarification, and an apology if appropriate, should be published as soon as reasonably possible by the Communications team.
- Respect other people's privacy. It is illegal to publish personal data about individuals unless they have given you their permission. As Council staff you are data controllers and will be personally responsible for anything you publish.
- In the event of an emergency situation, all scheduled social media output will be frozen to allow the communication officers running the crisis response to post critical messages. This will ensure clear communication between Buckinghamshire Council and the public until the emergency is resolved, and avoid the embarrassment of posting irrelevant or insensitive content in a time of crisis.

Political posts

- Our social media accounts must not be used at any time for political purposes such as campaigning, or trying to influence followers towards a certain political view.
- When using our social media accounts staff should not express personal or political views. Officers work to serve the administration and its goals, whatever political party is leading, and should remain neutral and not cross over into the political arena.
- When forwarding or sharing online messages, care should be taken that it does not appear that Buckinghamshire Council is endorsing a particular opinion.

Responding to comments and enquiries

- Assign customer enquiries to the relevant teams, either to answer them directly or to provide a response for use by the communications officer.
- Keep your communications clear, positive, polite and professional at all times.
- Avoid responding when incapacitated or otherwise tired and emotional.
- Respect the comments of those we don't agree with; allowing these comments to stay in our space is part of our objective of broader community engagement.
- Even if we disagree with a comment, all comments and messages should be responded to in a measured and friendly way.
- Don't argue with someone who is argumentative – some people like to row online for the sake of it.
- Generally, conversations should be carried out in the space in which they began – for instance, if a user comments in a public space, you should not attempt to move the conversation to a private inbox. However, exceptions may be made in the interest of reducing conflict, avoiding the further posting of offensive content, or where confidential information is being exchanged.

Removing content and blocking users

You should avoid blocking other social media users where possible, as this act in itself could result in a backlash that damages our reputation. However, while we have no problem with comments that disagree with or question Buckinghamshire Council and its actions, we will not accept content that is offensive or discriminatory. [Our Social Media Standards](#) have been published on the Buckinghamshire Council website and outline the acceptable use of our social media channels. Anyone who breaches these standards may be blocked.

- In the first instance, depending on the degree of offence, any unacceptable messages should be removed and, if appropriate, a private message can be sent to explain why this has been done.
- Content should only be removed if it is offensive, defamatory or you can show that it is in breach of this policy or breaks the terms of use that we have defined and made public ([Our Social Media Standards](#)). Social media respects and requires a democratic approach.
- If the same user/group continues to post offensive messages, there is likely to be grounds to block them. You should seek the advice of the Head of Communications before doing so.

- Racism, sexism, threats of violence, and any other forms of prejudice or harassment will not be tolerated and should be reported and removed.
- If you spot any sensitive Council-related information being leaked or shared on social media, you contact the relevant service area and Buckinghamshire Council's Data Protection Officer in the first instance.

FOI requests and complaints

Be aware that people may attempt make complaints and send freedom of information (FOI) requests using social media. There are statutory timescales for the Council to provide answers, so it's important that you:

- Monitor social media for FOI requests and complaints.
- Acknowledge the person attempting to submitting the FOI request or complaint, explaining what happens next.
- Ensure that any FOI requests or complaints are fed into the correct system and logged for response via the Council's formal procedure.
- Encourage any customers making a service request (rather than corporate complaint) to report it via the correct channel, rather than Council social media channels.

Personal information and confidentiality

- Social media communications must be compliant with our privacy policy and should not breach confidentiality.
- Personal information, whether that of an employee or customer, should never be published on social media.
- If a customer chooses to put their own details in a public comment – e.g. a benefits code or phone number – you should politely advise them to remove it and continue the enquiry through private messaging if possible.
- Publishing any internal material, such as a report or minutes from a meeting which has not already been made public, would also be a breach of confidentiality.
- Staff and members should always ensure that information disclosed about the Council, partners or colleagues does not breach any confidentiality agreements.

Use of videos and images

When taking group photographs and videos for use on our social media platforms, you must adhere to the following:

- In the case of photos and videos that include groups, make it clear to those being filmed/photographed that the image/video could be used for online and offline PR purposes, providing the opportunity for those that don't want to be included to step out.
- Where photos/videos are of groups of school children, the school may have blanket consent from parents for images to be used, but this will need to be confirmed with the school contact.

- In cases where individuals are the focus of an image/video, consent forms will need to be signed. For children under 16 and those who are unable to understand consent, it will need to be given by a parent or guardian. If the group photo/video is of children, and those children are identifiable, completed consent forms will be needed.
- Consent can be withdrawn at any time.

Copyright

- When sharing images/videos or using information from a copyrighted source, you should be mindful that permissions may be legally required, as would be the case with printed materials. This can not only be dependent on the source itself but also on the copyright policy of the social media platform being used.
- Check with the copyright owner that you have permission to publish the content and offer to credit/acknowledge their copyright.
- When sharing material and media from third parties, you need to be confident that it comes from a trusted source.

Adverts and inappropriate content

Advertisements on Buckinghamshire Council social networking pages should be monitored to check that they are appropriate.

Closing an account

The closure or mothballing of an account should be carefully managed to ensure that the channel does not remain Council-branded but neglected. You should discuss the closure of an account with a senior manager before taking any action.

Misuse of social media

In certain circumstances, the misuse of social media can constitute a criminal offence or otherwise give rise to legal liability against you and Buckinghamshire Council. It may also cause embarrassment to us and our customers/residents.

Uploading, posting or forwarding a link to any of the following types of material on social media, whether in a professional or personal capacity, could amount to disciplinary action under the staff disciplinary policy (this list is not exhaustive):

- Pornographic material (writing, films, pictures, video clips).
- A defamatory statement about any person or organisation.
- Material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to the Council, its customers/residents or its staff.
- Confidential information about the Council or any of its staff or customers/residents (which staff do not have express authority to disseminate).
- Any other statement which is likely to create any liability (whether criminal or civil, and whether for the member of staff or the Council).

- Material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

Any such action will be addressed under the [Buckinghamshire Council Disciplinary Policy and Procedure](#)

How content is monitored and moderated

You should be aware that any use of social media channels (whether for work or personal purposes) may be monitored and, where breaches of this policy are found, disciplinary action may be taken.

Where evidence of misuse is found a more detailed investigation may be undertaken in accordance with our Disciplinary Policy and Procedure. This may involve the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses involved in the investigation. If necessary, such information may be handed to the police in connection with a criminal investigation.

If you notice any use of social media by other staff or councillors in breach of this policy, you should report it to the Communications team.

4. Security

Passwords

If the wrong person gained access to Buckinghamshire Council's social media accounts, they could instantly contact thousands of residents with the potential to cause huge reputational damage.

The same security precautions around passwords should be applied to social media as they are to IT security in general, but with some differences and exceptions:

- Passwords should be issued by the Communications team and stored securely.
- Passwords should be changed regularly for security.
- Different, complicated passwords should be used for each account.
- Multi-factor authentication with the highest available privacy setting should be used where possible.
- Passwords should ideally be stored in a restricted folder that only authorised staff have access to.
- In the case of corporate social media, sharing passwords is unavoidable and, in contradiction to our IT Acceptable Use Policy, limited sharing is necessary.
- If it is necessary to share a password then it must be sent in an encrypted document, with the password to the document sent separately and ideally via a different channel such as WhatsApp. You should not share passwords through unencrypted messages or emails.
- Following a security breach or the departure of an employee with access, the Communications team is responsible for changing passwords and remotely logging

off all mobile devices that otherwise connect automatically. The method will vary depending on the channel.

Spam, viruses, scams and hacking

- Report accounts that appear to be bots, fake news channels, or other channels where the purpose is to spam users or spread viruses and other malicious content.
- Do not open messages or click links from accounts that you suspect may be used for such purposes. Just delete the message or report the post, and report the account to the relevant social media site.
- Avoid posting any details that might allow a hacker to guess our security questions or password.
- Do not log into Buckinghamshire Council social media accounts while using public Wi-Fi. These networks are often unsecured and our information could be stolen.
- You should also try to stay up to date on the latest scams and malware threats.

What to do if our social accounts are hacked

Being hacked is quite rare but if this does happen there are steps you should take:

- You should immediately alert the Communications team.
- Officers in the Communications team should report the breach to the relevant social media site before alerting the Service Director for Policy and Communications.
- If the account can still be accessed, the password should be changed immediately by the Communications team. A post should be sent out alerting our followers to the breach, and any posts published illicitly should be deleted.
- If the account cannot be accessed, the procedure of reporting the hack to the relevant social media site should be pursued by the Communications team.
- In instances when the hacked account cannot be accessed, the Council's other uncompromised social media channels can be used to alert the public.

5. Personal use of social media

The personal use of social media can sometimes be beneficial to organisations but there are some grey areas which have the potential to cause problems for both you and Buckinghamshire Council. This section aims to offer some clarity on this.

General

- We respect the desire to use social media for personal communication and expression, and ask you to exercise simple good judgement and common sense around how personal comments or activities online could reflect on the Council. This applies even if you are not apparently acting in an official capacity or identifying yourself as a member of staff.

- The same standards of behaviour and conduct apply online as would be expected offline. Our [Code of Conduct](#) for staff still applies.
- Employees should not engage in activities on the internet which might bring the Council into disrepute, and should not post derogatory or offensive comments on the internet
- You should be aware that through the open nature of social media sites, it is possible for third parties to collate vast amounts of information.
- The public must be able to trust the integrity of our services. Our residents need to be confident that the outside activities of our staff do not undermine Buckinghamshire Council's reputation and that decisions are not perceived to be influenced by any commercial or personal interests.
- If you are contacted by the press about posts on your personal account that relate to Buckinghamshire Council, you should speak with your senior manager and communications before responding. The Communications team must be consulted with regard to all press contact.
- Minimise security risks by using strong passwords and changing them regularly. Protect your devices with a pin to restrict access and prevent misuse.
- Be mindful that social media sites are sometimes used to distribute malicious software or code.

Interacting with Buckinghamshire Council social media accounts from your personal accounts

We encourage all staff to be ambassadors of Buckinghamshire Council and, just as we welcome you sharing stories of our events and developments in a way that supports the organisation, we also appreciate you sharing and engaging with our social media content in a positive way.

If you see comments criticising Buckinghamshire Council, please do not step in to defend the organisation. Instead, alert the Communications team so they can issue a corporate response if appropriate.

Privacy

It could cause irreparable damage to our reputation if any confidential information was to be leaked on social media. Staff must not reveal confidential information about Buckinghamshire Council, including internal policy or discussions.

- Always presume any information you put online will be shared publicly.
- Select the most secure settings for any personal social media accounts and consider removing your place of work from your account, so that you are less likely to be identified as a Buckinghamshire Council employee.
- Don't let anyone else access your social media accounts.
- Check your privacy settings so that you understand who can see what you publish and who can view your personal information. Anyone who knows your name or username can search for you online so make sure you are happy with what people will see if they do.

- Do not discuss work-related issues on social media forums – they are not necessarily private.
- LinkedIn is different from most other social media platforms as it is professionally focussed and centres on your employment. Any content you post on LinkedIn will inevitably reflect on your place of work and must be professional at all times.
- Personal blogs, websites and social media must not be used to attack or abuse colleagues. Staff members should respect the privacy and the feelings of others at all times.

Social media and politics

- You are entitled to express your own political views outside of work, but please remember to adhere to the [Code of Conduct](#) and don't bring the Council into disrepute. However, if your role is politically restricted, this will also extend to your activity on social media.
- It may be possible to see which groups and parties you follow on social media, so consider following groups and parties from across the political spectrum.

Work friends and social media

- You're free to connect with work colleagues on social media but be aware that anything on social media that goes against staff policies, such as the [Code of Conduct](#), or shows evidence that policy is not being adhered to, will be dealt with accordingly.
- Always ensure that your privacy settings are set to the highest level but be mindful that any social media posts may still be viewable by your contacts' networks.
- It may not be appropriate to share work-related content, such as photos from private staff-only events. Staff should be considerate to their colleagues, should not post information when they have been asked not to, and should remove published information immediately if asked by a colleague to do so.

Conflicts of interest

- You are free to talk about your job online unless there are specific concerns about the nature of your role. You should discuss any potential conflicts of interest with your senior manager.
- Any potential conflicts of interest regarding your use of social media should be discussed with your line manager and/or a senior manager.
- If you are offered payment to produce social media posts for a third party this could also constitute a conflict of interest and must be discussed with a senior manager.

6. Use of social media by councillors

A number of councillors have their own social media accounts with which to communicate with residents, share their own views and connect with the community proactively. This enables councillors to listen to what people are saying and engage with them on an equal

footing, focusing on two-way communications rather than simply delivering messages via press releases and newsletters.

Given the high profile of councillors in representing local communities, there are some important points that need to be considered:

- Misuse of social media may be in breach of the [Code of Conduct](#) for members.
- Social media is a very public communication channel and, as a Buckinghamshire Council member, anything you post or share can reflect on yourself and the organisation both positively and negatively. It can also be shared in seconds to a huge audience and cannot be controlled.
- Your social media content is likely to be connected to your role as a councillor and, while some councillors try to make it clear on their social media pages that their comments are their personal views, it is rarely a defence for well-known public figures. Inevitably, your personal views will be associated with your position as a councillor.
- Ask yourself whether you would say the same thing at a public meeting or to a reporter as you would post on social media. It could well amount to the same thing and, once posted, you can assume it's permanent.
- Avoid engaging with someone who is argumentative.
- Social media content should be accurate, appropriate, respectful, must not be open to misinterpretation and must not breach copyright law. Any content which fails in this is likely to damage the reputation of you and the Council and could risk breaching the [Code of Conduct](#) for members.
- You must not disclose confidential Council information, documents you only have access to as a councillor, or information which has been told to you by a resident or other party in confidence (even if you try to anonymise by removing names). Privacy must be respected.
- The best engagement comes from posts that are clear, jargon-free and give useful or interesting information for your followers. Posts also have more impact where they are accompanied by a picture or video.

7. Further information

Additional useful information on social media use for staff and councillors is published by the [Local Government Association](#).

Anyone with questions on our social media policy or in need of further clarification should contact the Service Director for Policy and Communications.