Social Media Policy

Policy document

Version number: 1.0

Publication date: July 2021

Revision cycle: July 2022

Policy Owner: Corporation Secretary, and Communications Director

Approved by: Policy Management Board

1. Purpose and Background

The purpose of this policy is to assist all Ofcom colleagues in engaging appropriately and securely in online communications in a personal capacity.

All Ofcom colleagues are required to comply with this policy.

2. Social Media Capacity

As the communications regulator, and as a public body, our independence, impartiality and integrity are central to the work that we do. It is essential that, as individuals, we uphold this reputation, act in ways that are consistent with Ofcom's values and maintain high professional standards. There should never be any legitimate reasons for external observers to question whether our advice or decisions might be influenced by our private interests or political opinions.

Social media is part of everyday life. Many Ofcom colleagues will have a personal presence on social media, networking and communications platforms. This policy is intended to balance our individual right to freedom of expression with our responsibilities as Ofcom colleagues. It seeks to set out underlying fundamental principles rather than being unduly prescriptive, but all Ofcom colleagues are required to adhere to this policy. To ensure that we maintain our reputation for impartiality, there are additional requirements if you are a colleague involved in broadcast standards enforcement or policy, deal extensively with external stakeholders[1] or are a member of the Senior Leadership Group.

This policy is not designed to discourage or unduly limit colleagues' personal expression or online activity - you are perfectly free to express yourself on subjects that are not matters of public, political, industrial or Ofcom-related controversy. We also encourage colleagues to share the work

[1] External stakeholders include Government, Ministers, companies regulated by Ofcom and/or members of the public with whom colleagues communicated in the course of their day-to-day role at Ofcom.

posted on official Ofcom social media channels, whether it's a project you've worked on, celebrating colleagues' achievements or initiatives that are important to you. The policy is designed to protect you and Ofcom from criticism that might arise from your engagement online.

Colleagues should note that any breaches of this policy may lead to disciplinary action. This policy does not form part of your contract of employment and Ofcom reserves the right to update it at any time. This policy does not apply retrospectively to personal expression or online activity in the past.

If you have any questions in relation to the content of this policy, please contact the Governance & Accountability team or the Communications team. If you have any queries either in relation to its implementation and/or how it applies to you, please contact the People & Transformation team.

2.1 Who does this policy apply to?

Social media / online platforms can be defined as 'websites and applications that enable users to create and share content or participate in social networking'. The following is a non-exhaustive list of platforms which this policy applies to:

- blogs;
- social and professional networks (such as Twitter, Facebook or LinkedIn);
- forums (such as Reddit or Mumsnet); and
- image and video-sharing platforms (such as YouTube, Instagram, TikTok or Twitch).

The policy does not apply to private messages, provided that you are not using the platform for business purposes. However, colleagues should be mindful of the principles of this policy and the potential for unintended onward dissemination of any views to a wider audience. Hints on staying secure online can be found at (link).

Ofcom has official accounts on the following social media platforms: Twitter, LinkedIn, Facebook, YouTube and Instagram.

2.2 Personal Communications

Remember that Ofcom is impartial. Ofcom as an organisation is, and must be, scrupulously impartial. Much of our work has implications for public policy or is the subject of political debate. Our impartiality, independence and objectivity are crucial to the work we do. For personal (i.e. non-business focussed) social media and online communications, Ofcom should not be included in your username, description, handle, or anywhere else on your personal social media or online profile, as this can imply that you are communicating in an official capacity on behalf of Ofcom.

Personal or Ofcom? On social media, the lines between public and private, personal and professional are blurred. Even where you do not state on your social media or online profiles that you work for Ofcom, other people might still be aware that you do. Disclaimers in personal profiles such as "my views, not Ofcom's" do not provide a justification for posting personal expressions of opinion that conflict with this policy. This is especially true if you are a colleague involved in

broadcast standards enforcement or policy, deal extensively with external stakeholders[2] or are a member of the Senior Leadership Group.

You should not post comments or engage in online conversations relating to:

a) Information relating to an ongoing regulatory matter (consultation, enforcement or compliance). You can only share outcomes after they have been published;

b) Legal matters, litigation, or reference to any parties Ofcom may be in dispute with (or with whom a legal or other dispute is contemplated). Do not comment on any ongoing public disputes Ofcom may be involved in;

c) Statements and opinions relating to court injunctions or other matters covered by reporting restrictions. Breaching a court order is a Contempt of Court, which is a serious offence potentially punishable by imprisonment, a fine, or both;

d) Non-public Ofcom information, including organisational announcements.

Conflicts of interest. Colleagues should adhere to the principles set out in the Conflict of Interest Policy (including the 7 principles of public life, also known as the Nolan Principles, which apply to anyone who works as a public office-holder) and apply the same standards set out in that Policy online, as well as offline, whether you are acting in an official or personal capacity. When a colleague is personally affected by a specific matter which may raise a conflict with the Conflict of Interest Policy, this must be declared to the People and Transformation team at the earliest opportunity. If in doubt, consult your line manager.

Political views. As we note in our Conflict of Interest Policy, to comply with Ofcom's status as an independent regulator, it is inappropriate for any colleague to engage in active politics in support of a registered political party, including active and visible political campaigning. Although acting as a Parish Councillor is acceptable and lower profile political activities may be permitted, colleagues must exercise their judgement when using social media to reflect their personal political views. In relation to issues that fall within or are associated with Ofcom's remit, no colleague should publicly express views on any policy which is the subject of current political debate or on any relevant public policy, political, industrial or Ofcom-related matters of controversy.

If you are a colleague involved in broadcast standards enforcement or policy, deal extensively with external stakeholders[3] or are a member of the Senior Leadership Group, there are additional requirements to ensure that we maintain our reputation for impartiality and that external observers have no reason to suggest that our advice or decisions might be influenced by our private interests or political opinions. Colleagues in these roles should not reveal how they vote or express support for any political party. They should also not express a view on any policy which is the subject of current political debate or on any relevant public policy, political, industrial or Ofcom-related matters of controversy.

---

[2] External stakeholders include Government, Ministers, companies regulated by Ofcom and/or members of the public with whom colleagues communicated in the course of their day-to-day role at Ofcom.

[3] External stakeholders include Government, Ministers, companies regulated by Ofcom and/or members of the public with whom colleagues communicated in the course of their day-to-day role at Ofcom.

Being decent. All colleagues, regardless of seniority, should behave appropriately online, in ways that are consistent with Ofcom's values. Colleagues should not post offensive or derogatory comments or content on social media. It is important to be respectful of others and ensure you do not say anything offensive in relation to protected characteristics. This includes someone's age, gender, gender reassignment, sexual orientation, disability, race (including nationality), religion and culture. You must not abuse your position as an Ofcom employee by criticising colleagues, stakeholders or Ofcom on social media; instead, please raise any concerns with your line manager or with the People and Transformation team.

Sharing controversial content. Remember that, if you share, like, retweet or engage with something controversial or objectionable on social media, there's a risk it might reflect badly on you – or on Ofcom. Take care to check the source, veracity and full content of any item that you are re-posting.

Protecting copyright. Make sure that you do not breach copyright on social media, for example by using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce something.

2.3 Business-focused networks

Business networking services like LinkedIn work best where professional details are shared. If you are on LinkedIn, you are likely to identify yourself as an Ofcom employee.

We always encourage colleagues to post about the work that Ofcom has published or announced, either on your own initiative, or as noted above by sharing the content posted on Ofcom's official social media channels.

For the avoidance of doubt, however, the same rules apply to your use of business networking services as apply to personal communications set out above (save that you are permitted to identify yourself as an Ofcom employee on business networking sites).

3. Version history

Version	Date	Revised by	Summary of changes
1.0	28/07/2021	JG & SR	Created

A1. Staying Secure Online

a) **Login details.** Do not use your Ofcom email address or password for any personal social media profiles – including LinkedIn. This can compromise the security of your Ofcom account.

b) **Confidential information.** Never disclose confidential information on social media. All colleagues have a duty of care to protect information held by Ofcom and must not disclose it externally without authority. That applies to social media too. Similarly, you should never express views on social media that are informed by confidential information relating to your work at Ofcom. You can find more guidance about this on the Information Security pages on the NewsHub.

c) **Staying safe and secure.** These tips will help you stay safe on social media sites. You should also look out for security updates on the NewsHub that will keep you informed about malware, phishing and other security concerns.

i) Make sure your email account is secure. Anyone who can read your emails can also access your social media accounts associated with that email address.

ii) Pick a strong password, and change it every few months:

- Use a different password for every site you visit
- Select strong passwords, with 10 or more characters, that can't easily be guessed
- Think of a meaningful phrase, song or quote and turn it into a complex password, using the first letter of each word, rather than using a word from the dictionary
- Randomly add capital letters, punctuation or symbols
- Swap numbers for letters that look similar (for example, "0" for "o" or "3" for "E")
- Never give your password to others or write it down
- You may wish to consider using a password manager. There are many free and pay options available.

iii) Keep personal information personal. Don't reveal your home address, phone number or email address in the bio/summary/equivalent section of your profile. The same could go for your professional contact details, too.

iv) Sign out of your account after you use a publicly-shared computer.

v) Keep your antivirus software up to date.

vi) Familiarise yourself with the privacy policies of the social networks you use.

vii) Know your friends and connections: if you don't know or have never heard of an account that sends you a request, it may be wise to ignore it. It could be a fake account.

viii) Consider turning two-factor authentication on for your social media accounts.

ix) Be careful what you click on. Always check the URL first and if the source seems suspicious, don't trust it - it may be a malicious link, for example phishing or malware.