Social media use policy

Version number: 2.0

Status: Published

Department/Team: External Communications and People Services

Relevant policies: Acceptable use policy, Dignity at work policy, Political activities policy

Distribution: Internal

Author/Owner: Rosie Kellett, People and Policy Manager and Kate Banks, Digital Social and Creative Content Manager

Consultees: External Communications, People Services, trade unions, REACH network, Women's Network

Approved by: Angela Balakrishnan, Executive Director Strategic Communications and Public Affairs, and Sam McVaigh, Director of People Services

Application date: 25 February 2026

Review date: 25 February 2028

Security classification: Official

Key messages

This policy aims to:

- promote respectful and proportionate use of social media, whether for professional or personal purposes;
- safeguard the ICO's independence, impartiality, reputation and business interests;
- prevent use of social media for prohibited reasons such as online harassment, discrimination or behaviour that could cause harm to others or the organisation; and
- set out how we will handle any misuse or breaches fairly and consistently.

Does this policy relate to me?

This policy applies to all employees, secondees, agency workers, contractors, non-executive directors and anyone else carrying out work on behalf of the ICO.

Table of contents

Introduction

Social media offers valuable opportunities to connect, share information, and engage with others. As the UK's data protection regulator and a public body, we must uphold the highest standards of independence, impartiality and integrity in everything we do. This includes how colleagues use social media.

This policy sets out the standards of behaviour we expect when you use social media in a professional capacity, or when your personal activity could reasonably be linked to the ICO. It's not intended to restrict your personal use, but to provide you with clear guidance for doing so responsibly.

It balances your rights to privacy and freedom of expression with our collective duty to maintain public confidence in the ICO's independence and impartiality.

We've designed this policy to safeguard:

- colleagues, third parties or other stakeholders;
- the ICO's confidential and private information;
- the ICO's compliance with legal and regulatory obligations; and
- the ICO's reputation and public confidence in our impartiality.

This policy applies to any website, application or messaging service that enables users to create, share or exchange content, or participate in networking or group communication (whether publicly or privately). This includes (but is not limited to) blogs, forums, and platforms such as Facebook, X, LinkedIn, Instagram, TikTok, Wikipedia, WhatsApp, Threads, BlueSky and YouTube.

'Content' includes written material or messages, oral communications, photographs, videos, visual images, music and information of any description.

If you have any questions about this policy or how it applies to you, please contact People Services via the Help App in Workday.

This policy is non-contractual. We may amend it at any time.

Back to the top

Using social media responsibly

Responsible use

When using social media, we expect you to:

- be responsible;
- exercise good judgement;
- use discretion; and
- ensure you respect others.

These principles apply to all your online activity, whether in a personal or professional capacity.

You're personally accountable for the content you publish. Even on private networks or messaging services, posts can be shared beyond their intended audience, so please consider how your content may reflect on yourself and the ICO.

You should always consider how your activity could be perceived by others and whether it could reasonably be linked to your professional role at the ICO.

You should:

- review privacy settings regularly to maintain control over personal information;
- refer to our guidance in the section Professional identification, when you disclose your affiliation to the ICO on your profile; and
- seek advice from your people manager or the External Communications Team if you're unsure whether a post or comment is appropriate.

Prohibited use

Certain behaviours present unacceptable risks to the ICO and are therefore prohibited. These rules apply to anyone working for or representing the ICO, and some continue after your working relationship with us ends.

Prohibited behaviours while working for the ICO

If you work for the ICO, you must not do any of the following:

- Engage in behaviour online that constitutes or could be viewed as illegal, bullying, harassment, discrimination, or impersonation of others, including colleagues or third parties.
- Post or share content that could damage our reputation, business interests or independence, or bring the ICO into disrepute, even indirectly. This includes defaming, disparaging or making false or misleading statements about the ICO, colleagues, clients or third parties.
- Disclose your clearance level on social media or public profiles, if you hold security clearance (eg SC, DV). This information is sensitive and sharing it outside secure professional settings may breach clearance terms and create a security risk.
- Post, share or endorse party-political content in a way that could reasonably be perceived as linked to your role at the ICO or as expressing an ICO position. You may express personal political views in a private capacity, provided you don't reference the ICO or present your views as official ICO positions or as being expressed on our behalf. You must take extra care during pre-election periods to avoid posts that could be misinterpreted as representing the ICO. You must follow the permission process for any activity that falls within the scope of our Political activities policy.
- Provide employment references or professional endorsements (eg on LinkedIn) on social or professional networking sites. Such references may be attributed to the ICO and create legal liability for both the author and the organisation. You must not present informal expressions of support or praise as an official employment reference on behalf of the ICO.

Prohibited behaviours during and after working for the ICO

While you work for the ICO and after your working relationship ends, you must not do any of the following:

- Post comments about sensitive business-related topics, such as our performance.

- Do anything to compromise our confidential information, sensitive operational details, or intellectual property, including sharing details of our cases, investigations, or internal operations.
- Leak confidential information about people or businesses obtained during your employment with the ICO. Doing so is an offence under section 132 of the Data Protection Act 2018. This duty exists independently of this policy and remains in effect after you leave the ICO.
- Use ICO logos, trademarks, or branding in any social media posting or in your profile on any social media without prior authorisation from the External Communications Team.

If any of your social media activity before your employment with us comes to light and we consider it breaches the standards set out in this policy, we may review the matter and take appropriate action. This could include disciplinary action, if the content impacts our reputation, impartiality or legal obligations.

Reasonable use during working hours

During working hours, you're permitted to use social media for personal matters for a reasonable amount of time that does not interfere with your work duties. For example, checking social media on a personal device during breaks is acceptable. However, you're not permitted to use it for a prolonged period of time that impacts your work responsibilities.

You're also not permitted to use ICO computers, devices, networks, or other IT resources and communications systems for personal social media activity. You must also comply with our Acceptable use policy when you use any ICO systems.

Back to the top

The ICO and your social media accounts

Separation of professional and personal activity

You don't need to reference the ICO in your personal social media accounts. However, even without an explicit reference, you may still be identifiable as an ICO colleague.

You should therefore consider how your posts, comments, and online behaviour could be perceived, and whether they might reasonably be linked to us.

In particular, you should consider any posts you make through your personal accounts that are public and can therefore be viewed widely. You may breach our policy if your posts:

- bring the organisation into disrepute (or are likely to bring the ICO into disrepute); or
- compromise our impartiality or reputation.

Mixed-use accounts

We recognise that the boundary between professional and personal social networking may sometimes be blurred. For example, a single use account that you use for both (eg if your LinkedIn profile includes your ICO role but also shares your personal views or non-work-related content).

Where this occurs, you must:

- exercise particular care;
- always apply professional standards; and
- ensure your posts remain respectful, accurate and consistent with our impartiality and independence.

Professional identification

You may state that you work for the ICO and include your role on professional platforms, such as LinkedIn.

However, you should consider whether it is necessary or appropriate to do so, and if there are any security implications. For example, if you're involved in high-priority investigations, it may not be advisable to share details of your role. You can get further advice from the Cyber Security Team.

Where you disclose your affiliation to the ICO, you must reflect the professional image we expect of an ICO colleague in your profile and content.

Using personal accounts for work-related activity

You may use personal accounts for legitimate work purposes, such as following ICO channels or monitoring and engaging with relevant stakeholders. This activity must be relevant to your role and must not compromise investigations or our other work.

If, through this activity, you become aware of information relevant to our role as a regulator, you must escalate it to your people manager and the relevant team. Likewise, you should report any social media content that disparages or reflects poorly on us or your colleagues.

Back to the top

Speaking on behalf of the ICO

You should read this section alongside our Acceptable use policy, which is particularly relevant if you use social media as part of your role.

Scope and authorisation

You may only post, comment, or respond on our behalf using professional accounts, if you're authorised by the External Communications Team. You're only authorised to post, comment, or respond on our behalf via our corporate accounts, if you're a member of the Social Media Team.

You must not create or manage new ICO social media accounts, pages, blogs, or channels.

Speaking on behalf of the ICO

If your role requires you to represent or speak on our behalf on social media, you must first obtain approval from your people manager and the External Communications Team.

You may be required to complete training or comply with additional guidance before posting.

You must refer any external requests for comment about us, including from journalists or for publication on social media, to the External Communications Team.

You must not respond directly or acknowledge these requests without written approval from the External Communications Team. This ensures all our public communication is accurate, consistent, and aligned with our values and regulatory obligations.

Back to the top

Online harassment and reporting

Reporting

Harassment of any kind via social media is unacceptable. We take all reasonable steps to safeguard colleagues and take appropriate action if and when this behaviour occurs and is reported to us.

If you experience harassment, including sexual harassment, bullying, derogatory, or abusive comments through social media in connection with your work or from ICO colleagues, you should report it to your people manager. Where this is not appropriate, you should escalate the issue to another senior manager.

You can find guidance and support in our Dignity at work policy.

Monitoring and escalation

If the External Communications Team becomes aware of a derogatory social media post naming an ICO employee, they will inform the employee's people manager and People Services.

The manager will discuss the incident with the affected employee and consider appropriate support or escalation. This could include reporting the post to the social media platform if it breaches their guidelines or community standards.

In some cases, the Information Security Manager may need to review the content to determine whether we should refer it to the police or other authorities.

Proactive organisational safeguards

We recognise that social media platforms are constantly evolving, and new technologies, including AI-generated content, can amplify risks. We keep our use of social media channels and emerging online risks under review, and take proactive steps to mitigate potential threats to colleagues' wellbeing and safety wherever possible. These safeguards are in addition to the reporting routes and escalation processes outlined above, and you're not expected to manage these risks alone.

Back to the top

Breach of policy

Any breach of this policy may result in disciplinary action up to and including dismissal. We will investigate all breaches in accordance with our Disciplinary policy and procedure.

Breaches apply to activity both on personal and corporate social media accounts that relate to our work or could affect our reputation.

You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may result in disciplinary action.

If you're unsure whether your social media activity complies with this policy, ask your people manager for guidance.

Back to the top

Version history

Version	Changes Made	Date	Made by
0.1	First draft	May 2018	Human Resources
0.2	Second draft	March 2019	Margaret Wilson-Savage
1.0	Approved and published	March 2021	HR, TU and EDI networks
2.0	Full policy review conducted. Policy transferred to new template.	February 2026	People Services (Rosie Kellett) and External Communications (Kate Banks).

Back to the top