



Social media policy

Policy sections



1. Introduction



2. Your responsibilities



3. Principles for use of social media



4. General standards



5. Engaging on behalf of the Improvement Service



6. Engaging on your own behalf



7. Managing your digital identity



8. Contact

1. Introduction

Social media offers new channels for engagement and collaboration within, and more importantly beyond, our own organisation. Increasingly a significant majority of people and organisations simply expect to be able to engage with other organisations and public bodies on platforms like X and Facebook.

In promoting the work of the Improvement Service (IS) it makes business sense to have a presence on a number of different social media platforms and to focus on the same channels used by partners and stakeholders.

Many IS staff will already be using social media in a variety of ways in their lives outside the office. This policy relates to staff use of social media as part of their work and sets out general standards that apply to all staff whenever their online activity could be connected to the IS.

To support staff in their use of professional and personal social media accounts, the IS will:

- provide training and guidance wherever possible to help you to make the most effective use of social media
- make it as simple as possible to access social media facilities from our network and remove barriers where appropriate
- support staff who use social media as part of their professional development

2. Your responsibilities

Using social media in your professional capacity as an IS member of staff, or even in a personal capacity if you identify yourself as an IS employee, puts you in the position where you can affect the organisation's reputation. Staff are therefore expected to adhere to basic standards. You are encouraged to share what you are doing to progress the work of the IS, but you must also respect that the IS needs to protect its reputation, information and systems.

Because there is a risk of reputational damage or even security breaches as a result of improper social media use, the IS expects staff to approach any use of

social media platforms responsibly and when making any social network postings you must:

- not create, film, record, post or upload any videos, images or other content in the workplace or on Company premises
- avoid posting disparaging or defamatory statements about the IS, your colleagues and stakeholders
- avoid social media communications that might be misconstrued in a way that could damage the Company's reputation, even indirectly
- make it clear that you are speaking on your own behalf
- if you disclose you are an IS employee, also state that your views do not represent Company views. You should also ensure that your profile and any content you post are consistent with the professional image you present to colleagues and stakeholders
- as you are personally responsible for your communications on social media, remember that what you publish might be available to be read by the masses (including the business itself, future employers and social acquaintances) for a long time

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss this with your line manager.

You will be expected to disclose to the Company any external or online activity that generates, or may generate, commission, payment or other financial or reputational gain before undertaking or continuing such activity. The Company reserves the right to withhold or withdraw permission where it reasonably believes the activity conflicts with its interests, interferes with your duties or performance, or poses a risk to its reputation or confidentiality.

In addition to the above:

- social media use should be documented as part of the wider communications plan and should involve discussions with the Communications Team
- staff should take care when sharing information or data on social media that it is accurate and that there are no restrictions on its use in a public forum
- staff are expected to comply with [GDPR legislation](#) as well as the IS's own [Information Security Policy](#) and [Privacy Notice](#) when sharing information on social media

- the Communications Team may ask staff to assist in monitoring the IS's use of social media platforms including measuring and reporting on the effectiveness of social media activity

3. Principles for use of social media

These principles are intended to underpin the use of social media across the Improvement Service. They are not listed in any priority and should be regarded as mutually reinforcing. They should not be seen as detracting from or supplementing existing legal obligations regarding access to information and consultation. For guidance on personal use and the general standards that apply to all staff, see sections 4 and 6. There is also advice on engaging in social media on your own behalf and how you might want to differentiate between your personal and professional online activities.

The [Improvement Service Values](#) are fundamental to all the work that we do, and this includes anything which is shared on social media. All staff should take care to do nothing online that would damage the IS's reputation.

- **Be professional.** Remember that you are acting as a representative of the IS on official channels
- **Be transparent.** If you are speaking in your professional capacity, disclose your position as an employee of the IS and make it clear if you are speaking in a purely personal capacity
- **Be credible, accurate and fair.** Libel, defamation, copyright, freedom of information and data protection laws all apply to social media content
- **Be integrated and inclusive.** Make every effort to be accessible and connect with all relevant communities. Write in plain English and ensure that videos are captioned and that you add written descriptions to images where appropriate
- **Be accountable.** You are responsible for what you say online. You cannot cover up mistakes and can only seek to correct them
- **Be proud of your professionalism and hard work.** You should take pride in the professionalism and hard work that you and your Teams put into delivering IS projects and services but personal commentary – positive or negative – is not appropriate on official channels

- **Be responsive and respectful.** Visit frequently the online spaces where you have a presence and respond promptly to the conversations. Always pause and think before posting. Do not engage in online arguments through official social media channels and do not respond to abusive posts. Abusive posts should be reported to the Communications Team and to the social media channel on which they appear
- **Be careful.** Never give out personal details like your home address or phone number

Remember:

- anything you post online is open to being republished in other media
- you may attract media interest in yourself as an individual, so proceed with care whether you are commenting in a business or a personal capacity. If you have any doubts, take advice from your line manager or the Communications Team

4. General standards

As an member of staff, you must take the following into consideration when using social media in any capacity – personal, for professional development, or officially on behalf of the Improvement Service.

- if you are acting in your official capacity then make this clear and identify yourself and your role
- ensure your profile and related content is consistent with how you wish to present yourself with colleagues, customers and stakeholders
- be aware of your language and conduct. As in all cases where you are speaking in public, you should be aware of libel, defamation and slander. Take care not to post or share content which could be understood as running counter to the IS Values on Equality and Diversity
- never share confidential or sensitive information. You should know and follow the rules on confidentiality and official information
- try to add value. Provide worthwhile information and perspective. The Improvement Service is best represented by its people and what you publish will reflect on the wider organisation

- if you're about to publish something that makes you even the slightest bit uncomfortable, don't shrug it off and hit 'send.' Review these guidelines or discuss the content with the Communications Team with a view to identifying and resolving any potential issues
- if you wish to participate on social media platforms in a professional capacity, discuss it with your line manager and the Communications Team
- if you think you may have made a mistake, admit it in the same forum. Be upfront and be quick with your correction. IS Values require staff to be accountable and this includes any mistakes you may make. Alert your manager or your Communications Team as soon as possible in the event that you make a mistake
- if you mistakenly publish something sensitive or restricted inform your line manager and the Communications Team as soon as possible. Even if it has been deleted, the information could still be online
- it can be easy to start or get involved in a controversy unintentionally. If you find that one of your social media posts has created a firestorm, inform your line manager and the Communications Team immediately

5. Engaging on behalf of the Improvement Service

Social media is about the social connections and conversations we have with our service users, stakeholders and colleagues. To gain the maximum value from these tools, you should look to foster relationships. Therefore, you will need to acknowledge and understand the commitment and investment of time in building and developing sustainable online relationships.

- understand the resources available to you to maintain and foster sustainable relationships
- think through why you are using social media and what outcome you wish to achieve. For example, if you are inviting public responses then think through how you will use the results and how this fits in with other forms of consultation
- think through potential risks and have plans in place to manage and mitigate these

- respect your target audience. Think about their specific needs and be aware of language, cultural or other sensitivities you may need to take account of
- seek permission to publish any information, report or conversation that is not already in the public domain. Do not cite or reference customers or stakeholders without their approval
- respect copyright when linking to images or other online material
- stay within the legal framework and be aware that data protection and financial regulations apply
- discuss with the Communications Team how you intend to monitor the success of social media activity

6. Engaging on your own behalf

There are a number of benefits to social media, both for organisations and individuals. When you are not at work, it is entirely up to you to decide whether and how you choose to create or participate in a social media space or any other form of online publishing or discussion. The views and opinions you express are your own.

If your online activity could reasonably be linked to the IS, the standards in this policy apply (see sections 2 and 4)

As an Improvement Service member of staff, it is important to be aware that posting information or views about the IS cannot be isolated from your working life. Any information published online can be accessed around the world within seconds and will be available for all to see.

- you are personally responsible for any content you publish
- review your privacy settings and understand who can see the information you publish
- do not let your personal use of social media interfere with your job or your work/life balance. If your use of social media is affecting your mental health, take a break or delete your account and seek help from one of the mental health first aiders at the IS

7. Managing your digital identity

Be mindful of the personal information you disclose on social media sites, especially with regards to identity theft. Making information such as your date-of-birth, your place of work, and other personal information publicly available can be high risk in terms of identity theft.

- review and use privacy settings. Most major social media sites allow you to control how visible your information is on the site. You need to decide how visible you want your contact and profile information, videos, photos, and other posts need to be, and take the time to set the appropriate controls within the media site in question
- on most social media sites, you can limit who can see photos or video tagged with your name. You should consider how appropriate any video or photos are before you upload them. You also need to take advantage of any settings that allow you to control how visible this content could be if your friends have not exercised such good common sense
- be especially careful of malicious links sent via social media accounts. In general resist the urge to click on links sent to you no matter the source
- protect social media accounts from being hijacked. Use strong passwords and never disclose those passwords to another person

8. Contact

If you have any concerns or issues about using social media, want to discuss any aspect of this policy, or any additional aspects of using social media within the Improvement Service, please make contact with any member of the Communications Team.

