Social media policy

Document name/title	Social media policy
Version number	V1.0
Status (draft, published or superseded)	Published with trade union approval
Department/Team	Human Resources
Relevant or related policies	Managing customer contact guidance. Acceptable use of IT policy.
Distribution (internal or external)	Internal
Author/Owner (if different name both)	Human Resources
Approved by	SLT and Trade Unions
Date of sign off	April 2021
Review by	December 2023
Security classification	Official

1. Scope

This policy applies to all employees, agency staff, secondees, contractors, non-executives and other workers of The Information Commissioner's Office.

2. Purpose

2.1 This policy is in place to promote responsible usage of social media whilst minimising the risks to our business through inappropriate use of social media; inform staff of their obligations with regard to the use of social media; and to enhance the continuing development of the ICO through insight and intelligence gleaned through social media channels.

2.2 This policy deals with the use of all forms of social media, such as Facebook, LinkedIn, Twitter, Wikipedia, Whisper, Instagram, WhatsApp, Tik Tok, YouTube and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time and any changes will be communicated to staff prior to becoming effective.

2.4 The purpose of this policy is to inform staff of their obligations with regard to their own use of social media. If any member of staff, when dealing with ICO customers, is subject to harassment or derogatory comments via social media, they should bring this to the attention of their line manager or a more senior manager as appropriate.

2.5 Should the ICO Communications team come across a derogatory social media post that refers to an ICO employee by name, they will inform the employee's line manager. The norm would be to discuss the post with the affected employee, however this will be considered on a case by case basis. The post will be reported to the social media platform. The employee's line manager will deal with the customer's complaint following the same procedures for offline communications. It may also be necessary to provide a copy of the post to the Information Security Manager, who will assess if the nature of the content justifies informing the police or other relevant authorities. Further guidance on dealing with challenging customer behaviour can be found in the Managing Customer Contacts guidance on ICON.

3. Roles and responsibilities

3.1 Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with Human Resources who will review this policy periodically to ensure that it meets legal requirements, draws upon best practice and reflects developments in social media use and technology.

3.2 Managers have responsibilities for the effective implementation of this policy. This includes ensuring that their team members are given the opportunity to read and understand the policy and are aware of the standards of behaviour expected. Managers are not expected to monitor social media use from their team members, but are expected to take action when they are made aware of behaviour which falls below the level required.

3.3 All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it, adhere to the requirements described and ensure that their use of social media involving reference to the ICO does not damage the reputation of the office.

3.4 Any misuse of social media should be reported to the relevant member of staff's line manager and in turn to the Head of HR. Questions regarding the content or application of this policy should be directed to Human Resources.

4. Personal Use of Social Media

4.1 Unreasonable use of social media for personal matters is not permitted during working hours or by means of ICO computers, devices, networks and other IT resources and communications systems. This could potentially lead to disciplinary action.

4.2 It is recognised that you may wish to monitor social media channels for work purposes via a personal account, for example following the Twitter feeds or Linked-in postings of the ICO or relevant stakeholders. This can provide the organisation with useful insight into how we are perceived and how we can develop our services.

4.3 Such monitoring must be relevant to your work, and must not compromise any investigations or other activities undertaken by the ICO. It must not negatively impact on the time you spend on your

core duties or be a mask for personal use of social media in work time. If you become aware of matters which are relevant to the business of the ICO through social media monitoring, you should raise the issue with the relevant ICO manager.

4.4 For social media sites or applications which are solely work or professionally based, such as LinkedIn or professional networking forums, you are permitted to state that you work at the ICO, and the capacity of your employment. Before doing so, you should consider if this is relevant or necessary, and if there are any security implications of doing so. For example, if you are involved in high priority investigations it may not be advisable to provide details of your role. Further advice is available from Cyber Security Team. Where your social media accounts are for personal use only, you do not need to say that you work for the ICO.

5. Prohibited Use

5.1 You must not make any social media communications that could damage our business interests or reputation, whether directly or indirectly.

5.2 You must not use social media to defame or disparage the ICO, our staff or any third party; to harass, bully or unlawfully discriminate against staff or any third parties; to make false or misleading statements; to directly or indirectly make derogatory comments or use offensive or inappropriate language in any social media communication; or to impersonate colleagues or third parties.

5.3 You must not express opinions or provide advice on behalf of the ICO via social media, unless expressly authorised to do so by your manager. You may be required to undergo training in order to obtain such authorisation.

5.4 You should note that if you provide advice on social media in a personal capacity on matters which relate to the ICO's responsibilities, it is often easy for you to be identified as connected to the ICO. Therefore your advice may be interpreted as reflecting an official ICO line. You should therefore avoid exposing yourself to a situation where your advice or views could potentially be interpreted as those of the ICO. Speak to your manager as soon as possible if you think that there is a risk that this may have occurred.

5.5 You must not post comments about sensitive business-related topics, such as our cases or performance, or do anything to jeopardise our investigations, confidential information and intellectual property. You must not include our logos or other

trademarks in any social media posting or in your profile on any social media.

5.6 You are reminded of your duty of confidentiality to the ICO and the requirements of s.132 of the Data Protection Act with regard to inappropriate disclosure of information. This duty continues after you leave the ICO. You are also reminded of your contractual obligation not to undertake any activity which may embarrass the public image of the Information Commissioner.

5.7 Any misuse of social media should be reported to the relevant member of staff's line manager and in turn to Human Resources and may result in disciplinary action in accordance with the ICO's disciplinary policy. Disciplinary sanctions will be as described in the disciplinary policy, up to and including dismissal, depending on the nature of the misconduct identified. Examples of what may be regarded as gross misconduct include (but are not limited to): posting derogatory or offensive comments about the ICO, colleagues, or customers; the deliberate or negligent disclosure of information about the ICO's activity; and the posting of comments which may cause harm to the reputation of the ICO.

6. Business Use of Social Media

6.1 If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from your manager. Your manager may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

6.2 Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to Corporate Communications and do not respond without written approval.

7. Guidelines for Responsible Use of Social Media

7.1 When making personal use of social media, (ie you are not posting in your capacity as an ICO employee) you must not imply that you are posting on behalf of the ICO, or as a member of ICO staff. Write in the first person and use a personal email address.

7.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone

to see. On personal social networks and messaging services– even closed ones like Facebook and WhatsApp – you should be aware that posts can be shared outside of your network. If you make a posting which could bring the organisation into disrepute then you could be subject to disciplinary action.

7.3 If you disclose your affiliation with us on your business based social media profile or in any social media postings, you must state that your views do not represent those of your employer (unless you are authorised to speak on our behalf as set out in section 6). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

7.4 You should be aware that it is possible for social media users to connect the work you do for the ICO with other social media postings. The likelihood of this is increased if you declare on business based social media that you work at the ICO. It is therefore important to remember that when posting in a personal capacity you may still easily be identified by other users as working for the ICO even if you don't state it.

7.5 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

7.6 Alerting Corporate Communications if you come across postings which are negative about the ICO will help the team to understand perceptions of the ICO, and manage our reputation on social media if responses are required.

7.7 The privacy settings on social media apps and websites should give you control over how your personal information is used. All staff who use social media are advised to check their privacy settings before using a particular service and to review them regularly, particularly after any new settings are introduced.

8. References

8.1 Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

9. Monitoring

9.1 We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems including but not limited to social media postings and activities. This may be done for legitimate business purposes which include ascertaining and demonstrating that expected standards are being met by those using the systems and for the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime).

9.2 For further information, please refer to our Acceptable Use of IT Policy

10. Breach of this Policy

10.1 As stated in Section 5, breach of this policy may result in disciplinary action up to and including dismissal. All breaches will be investigated in accordance with the ICO Disciplinary Policy and Procedure and the level of disciplinary action to be taken, if any, will be a matter of judgement for the chair of the disciplinary hearing.

10.2 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 in itself result in disciplinary action.

11. Frequently Asked Questions

11.1 Can I declare on social media that I work for the ICO?

Yes, if it is a professional based social media platform, but ensure you reflect a professional view of yourself and the organisation in all your postings. You should be aware of the ability of people to connect your work role to other social media which you use on a personal basis. However, there is unlikely to be a need for you to say you work at the ICO on personal social networking sites.

11.2 What happens if I make a mistake when using social media?

How the ICO deals with particular mistakes will depend on the nature of the error and the connection to your work. You should always inform your line manager and the Head of HR and Facilities if you are at all unsure whether you have made a mistake on social media that may affect the ICO or its business and reputation. Your

conduct online is subject to the same disciplinary rules and the expectations of the staff code of conduct as your offline conduct.

However, steps you could take are:

- Delete the post and apologise for the mistake, explaining the material was posted by mistake.
- Inform your line manager and the Head of HR and Facilities for advice.

11.3 **Will the ICO actively search social media for information posted by members of staff on their personal accounts?**

No, unless information has been received that would require further investigation because it breaches ICO rules or standards of conduct.

11.4 **Does this mean that I can't post reviews, even positive ones, about working at the ICO on sites like Glassdoor?**

No, that's not the case. It is recognised that staff may want to make full use of opportunities offered by social media, and social media can be used to benefit the ICO. However it is important that employees protect the privacy, confidentiality and interests of the ICO, our services and our staff. As with any form of communication, if in doubt, seek advice or do not post at all.

11.5 **What should I do if a colleague is sending me unwanted messages or posting disparaging messages about me on non-work related social media pages?**

Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform their line manager who will then discuss the issue with HR.

Support and advice is available from resources such as HR, The Employee Assistance Programme and EDI networks.

11.6 **Why is the ICO concerned about things I might post on social media in a personal capacity?**

Boundaries between corporate life and private life can become blurred when using social media and as such employee's actions and posts have the ability to affect the organisations brand and reputation. It is important that employees are aware of the impact their posts could have on the ICO and should therefore use social media responsibly.

11.7 **Are messages received via WhatsApp, Messenger and similar applications covered by this policy?**

In principle all forms of social media and digitial communication are covered by this policy. This includes WhatsApp, Messenger etc. and indeed any new forms of social media or digitial communication that may be introduced or become popular in the future.

It is correct that in these instances only the sender and receiver(s) can see the content. However the content can in principle be widely distributed if it is transferred into other social media platforms. The fact that the content may be private, would not excuse otherwise unacceptable or inappropriate behaviour such as the sharing of derogatory or discriminatory comments about colleagues or third parties.

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 & EDI Networks