Policy Name

Implemented on	December 2018
Last review on	February 2022
Next review due on	February 2023
Policy owner (name)	[redacted]
Policy owner (division)	Digital Publishing
Main point of contact	[redacted]@ons.gov.uk
Published version link	

1. Scope

This policy covers using external social media channels as an employee and as an individual, with additional policy for internal forum Yammer.

2. Background

All civil servants are bound by the Civil Service Code. The Code sets out the core values of integrity, honesty, objectivity and impartiality – and the standards of behaviour that are expected of us whether we are online or offline, in work or personal time. It is important you are aware that posting any content online which is considered to be a breach of the Civil Service Code or ONS's code of conduct may result in disciplinary action (please refer to the Policy detail section for more info).

3. Policy statement

This policy seeks to provide clarity on what is and what is not appropriate for civil servants when using social media – on external-facing channels such as Twitter and Facebook – as well as a process to follow should a breach occur. It highlights the key things to remember; clarifies the boundaries and potential issues; and empowers employees to use social media responsibly.

4. Policy detail

Social media is an important means of communication with millions of people choosing to interact online. When using social media be responsible in your actions, respectful of others and clear about who you are representing.

Think before you post. Don't forget: if you wouldn't do it offline, don't do it online.

Five things to remember when using social and digital media, either at work or in a personal capacity:

i. Common sense – social media helps us work openly and connect with the citizens we serve, just remember to apply common sense!

ii. Adhere to the Civil Service Code – apply the same standards online as are required offline, whether acting in an official or personal capacity

iii. Doubts? – if in doubt, don't post it

iv. Accuracy – check the accuracy and sensitivity of your content before posting online

v. Permanent – remember once something is posted online it’s very difficult to remove it

ONS understands that you may be proud of where you work and want to include this on your profile, or talk about it with your friends online. However, if you have a personal social media page and share who your employer is, you should make it clear that your views do not represent your employer’s views. You should also be aware that even with a disclaimer, your views could still be associated with ONS.

You should avoid posting negative comments about people or work at all times. Be aware that content on social media may be used in disciplinary action or grievances against you.

If you are authorised by ONS social media team to represent the organisation online using the ONS corporate accounts, you should follow the principles highlighted in this policy. This applies at all times when representing ONS through an ONS branded account, on work or personal IT equipment. Ensure that you disclose and comment only on information for which you have authorised permission and ensure that the information which you are sharing is accurate and complies with departmental policy.

Information and passwords linked with corporate social media accounts belong to ONS and remain the property of ONS even after a person is no longer employed by us.

If you are not authorised to represent ONS but you use social media professionally (for example to network via a professional social media site) then you should again follow the principles highlighted in this policy. Consider the fact that when using social media in this manner it can be easier for your views to be misinterpreted as being those of ONS.

When identifying yourself as an ONS employee, consider if there are any potential threats to your personal security. Don’t take pictures of your ID badge, serial codes on IT equipment and share these online.

It is your responsibility to make sure that using social media in a personal capacity does not affect your ability to carry out your work with integrity, honesty, objectivity and impartiality.

As with any communication channel, problems can arise if you use social media inappropriately (either at work or in your personal time) and this may lead to disciplinary action being taken by ONS. Principles of inappropriate use and action taken could include:

Soft breach

i. Agree with external criticism
ii. Engage in broad ONS matters not specific to your job
iii. Suggest without evidence ONS is not a responsible or fair employer
iv. Staff should not share internal material (including photos of the office or grounds) on social media. Please see the Physical Security policy for more information.

Action taken in case of a soft breach:

- The person responsible for the breach should be contacted by their line manager with details of the breach. The social media team will provide any details they have been provided with by internal staff or by a member of the public (eg screenshots) of the breach. The social media team will provide guidance to the line manager on the appropriate use of social media – eg this policy and related Civil Service guidance – and the line manager should discuss this with their staff member.
- If there are repeated soft breaches by the same staff member, the line manager should discuss with an Employee Relations Casework Manager (raise a Service Desk call).

Hard breach

i. Question ONS's data security protocol or independence from government
ii. Vent frustrations, bully or harass users
iii. Post offensive, derogatory or inappropriate content
iv. Suggest or confirm ONS has been hacked
v. Create, increase or inform public of a security threat or incident
vi. Imply or confirm statistical content of any release before 09:30 publication

Action taken in case of a hard breach:

- The person responsible for the breach should be contacted by their line manager with details of the breach. The social media team will provide any details they have been provided with by internal staff or by a member of the public (eg screenshots) of the breach. The social media team will provide guidance to the line manager on the appropriate use of social media – eg this policy and related Civil Service guidance – and the line manager should discuss this with their staff member. The line manager will also need to discuss any appropriate disciplinary action to take with an Employee Relations Casework Manager (raise a Service Desk call).
- If appropriate, the social media team will contact the IT Security Officer to advise the best course of action for the breach itself.
- If appropriate, the team will alert the Deputy Director or Director for Digital Publishing of the breach.

It's worth noting what ONS does not deem as a breach:

- Commenting generally that work has been frustrating
- Weekend activities that - albeit seen as unsavoury by some - are the right side of the law
- Constructively highlighting flaws in the ONS website or the way products are presented

Don’t use public-facing social media as a channel to air your work-related grievances or issues. Please use appropriate channels. Once something has been said online, it stays online and this could result in reputational damage for yourself and ONS.

It is the responsibility of all employees to ensure online interactions stay within the law, for example defamation, copyright, equality and data protection laws.

Employees are required to fully cooperate with investigations into any alleged breaches of this policy. This may include providing information on, or access to, online material and removing online content when asked to do so.

Yammer

Yammer is an internal social media platform that allows colleagues across the organisation to interact with each other on work or personal activities.

The ONS Yammer platform only allows access to employees of the ONS, UK Statistics Authority and the Office for Statistics Regulation, and is therefore more secure than other platforms. However, content on Yammer could still be the subject of Freedom of Information requests, so care should be still be taken when posting content on Yammer.

Yammer is governed by the principles set out in this policy, but as it is an internal channel, is managed by the Internal Communications team. The team do not moderate in the same way they do other channels (ie Reggie) but action can be taken to remove content if it is deemed in breach of this policy or the Civil Service Code.

Any potential breaches on Yammer should be reported to the Internal Communications team.

More information on the appropriate use of Yammer can be found on Reggie

5. Roles and responsibilities

Role	Responsible for	Accountable to
Social Media Lead	ONS Social Media channels, ONS, Facebook and LinkedIn	[redacted] G6 Digital Publishing

All DP-owned social media accounts have two-factor authentication in place.

6. Supporting documents

Useful links

Employee Relations Policy

Civil Service Values and Standards of Behaviour

Social Media Guide for Civil Servants

IT and communications guide on Reggie

Intro to Social Media module on Civil Service Learning

Original social media policy with guidance for social media use