

DWP Social Media Policy

Contents

1. Introduction	1
2. Policy Purpose	1
3. Scope	1
4. Social Media abuse (including trolling, stalking and bullying)	2
5. Professional or personal use	2
6. Compliance and monitoring	2
7. Trade Union Activity	3
8. Further information	3
Annex 1	3

1. Introduction

1.1. Social media refers to all web-based tools which allow users to generate content and interact with each other online. Many of the technologies used are still developing and can often put individuals and organisations at risk of online abuse. It is mandatory that all employees and contractors adhere to this Social Media Policy and supporting Standards, which provide a practical approach to minimising these risks.

NOTE: For the purposes of this Policy, the term “social media”, relates to all online platforms involving user generated content, not just the more recognised sites like Facebook, Twitter etc. Review sites, chatrooms, forums and blog entries etc., (this list is not exhaustive) are also within the scope of this policy. “Content” includes unauthorised video and / or call recordings.

2. Policy Purpose

2.1. This policy and supporting Standards helps to ensure that all DWP employees and contractors (“users”) utilise social media in a responsible, safe and secure way.

2.2. The policy and supporting Standards define the boundaries between professional and personal use and in so doing, ensures that users understand the risks of using social media and how to minimise them.

3. Scope

3.1. This policy and supporting Standards applies to all DWP employees and contractors utilising social media platforms for official business via DWP Accounts, Individual Professional Accounts (IPA) or Personal Accounts (See Section 5 below for definitions) – the policy applies to both professional and personal use. This includes DWP managed devices and users’ personal devices, in both work and personal time where this relates to DWP business, or an individual’s responsibilities under the DWP Acceptable Use Policy / Standards of Behaviour Policy and The Civil Service Code.

3.2. This policy and the supporting Social Media Standards applies to new and existing social media accounts. All account holders/sponsors must ensure that any existing accounts are compliant with the requirements of this policy.

4. Social Media abuse (including trolling, stalking and bullying)

4.1. The Department will not tolerate the harassment, discrimination, or defamation (trolling, stalking or bullying – [see Annex1](#)) of users via social media. It will investigate any allegation of abuse directed at the Department's employees via social media platforms.

4.2. This would be defined as, but not limited to, abusive comments posted on social media sites, unauthorised video footage, telephone recordings etc. and applies whether the alleged action took place at work or in users' personal time.

5. Professional or personal use

5.1. Users must operate separate social media accounts for professional and personal content. In this instance "professional" is defined as use only for DWP business related activity. Any user activity, either professional or personal on social media platforms, must comply with the requirements of this policy as defined in section 6 below.

Account Definitions

Official DWP Accounts – accounts used for official DWP business to provide information and services to customers, stakeholders and the public.

Individual Professional Accounts (IPAs) – accounts used for posting, sharing, promoting or engaging with DWP related content – users must be officially approved and are representing the Department. Therefore, they must only use IPAs on DWP approved devices, unless an exception to policy has been granted.

LinkedIn accounts – accounts used for official networking which can be run from a user's DWP or personal device, but a personal email address must be used.

Personal Accounts – accounts used by individuals in their own time to engage in or post non-DWP related content.

5.2. Any business requirement that is not consistent with this policy must be raised with the Security Advice Centre (SAC) in the first instance and consideration should be given to the Security Policy Exception process if necessary.

6. Compliance and monitoring

6.1. Users are responsible for understanding their responsibilities as defined in this policy and the consequences of non-compliance. The Civil Service Code, the DWP Acceptable Use Policy and DWP Standards of Behaviour must be read in conjunction with this policy. Compliance to the policy and personal conduct applies to the use of personal social media accounts, as well as professional accounts.

6.2. Non-compliance or breach of this policy may result in disciplinary action being taken (as well as consideration of a criminal prosecution if appropriate) which could lead to dismissal.

6.3. DWP have the right to undertake routine monitoring to protect individuals and guard against any potential cyber-attack. The Strategic Communications Team and Service Excellence's Social Media Team analyse any reference or sentiment towards DWP. Any misuse of social media which is identified during this routine monitoring work will be reported to the Security Incident Response Team for investigation.

6.4. Failure to report a security incident, potential or actual, could result in disciplinary action.

7. Trade Union Activity

7.1. Trade Union members have the right to engage in trade union related debate and activities in their own time, using personal accounts and their own equipment as per existing guidance in the DWP Employee Relations Framework, the Civil Service Code and DWP Standards of Behaviour.

7.2. Official Trade Union account activity on official TU social media accounts is outside the scope of this policy. As such Trade Union related accounts may mention DWP in the account name e.g. PCS DWP Group Branch.

8. Further information

8.1. Please contact the DWP Security Advice Centre for further advice regarding this policy.

8.2. The DWP Social Media Guidance and DWP Social Media Standards provide more detail on how to Use social media responsibly, securely and safely.

Annex 1

Social Media abuse definitions

Internet Trolling

Internet Trolling is the act of bullying or harassment online by way of posting inflammatory and digressive or off-topic messages in an online community with the intent of provoking readers into displaying emotional responses, whether for the troll's amusement or a specific gain.

Cyberstalking

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel.

Cyberbullying

Cyberbullying or cyberharassment is a form of bullying or harassment using electronic means. Cyberbullying and cyberharassment are also known as online bullying.