SIRO NOTICE
Senior Information Risk Owner

2020/001

Social Media

SIRO NOTICES

SIRO Notices are Welsh Government notices of organisation wide changes to security related procedures that must be adopted by all Divisions. Deputy Directors are required to confirm, through their Directors, that the changes have been implemented in their areas via the annual Internal Control Questionnaire.

In the last fortnight, Welsh Government responded to a serious staffing and security incident over social media use. The First Minister subsequently requested an urgent review of Welsh Government social media use. Annex 1 details the incident and includes a well-publicised social media incident involving Wales Office.

Welsh Government Social Media Accounts (see Annex 2 for the full list)
Whilst SIRO notices are usually reserved for changes to security procedures, the investigation has shown poor practice that breaches policy in a number of areas. Consequently, **with immediate effect**:

- All use of Welsh Government social media accounts (Annex 2) must only take place using Welsh Government owned devices. All use of the accounts from personally owned devices will cease.
- No member of staff is permitted to change the registered email address associated with a Welsh Government social media account to a personally owned email address.
- Any Welsh Government social media password details that have been shared with third parties must be changed immediately. Third parties must not have access to passwords for Welsh Government social media accounts.
- Two factor authentication must be activated for all Welsh Government social media accounts where it is an option that can be configured.

Personally Owned Social Media Accounts
As a Welsh Government employee you must ensure that your activity on social media does not bring the Welsh Government in to disrepute. This responsibility is included in the Civil Service Code and our Security Policy along with details about commenting on politically sensitive matters in a private capacity.

Many members of staff regularly use their personal social media accounts for sharing or liking content which promotes the work of the Welsh Government. We do not wish to stop this activity, however, staff are reminded that any content that they post and their activity on these platforms is publically viewable.

It is apparent that a significant number of staff are using personally owned social media accounts to promote their role or activity as a Welsh Government employee.

Line managers must not persuade or pressure staff in to using personal accounts to promote Welsh Government business.

If I had a personal Twitter account and followed the poor pattern of some, my account profile might read something like:

*The below is an example of **bad** practice*

> 'Director Human Resources, Welsh Government. Tweets are my own views'.

Clearly, if I tweeted or liked a discriminatory or offensive post, the 'caveat' that tweets are personal views is irrelevant as they would be incompatible with my role and bring the Welsh Government in to disrepute.

Because of the widespread use of social media in this way, I am asking members of staff to **get in touch before the 28/02/20** if they are using personally owned and managed accounts as part of their role or to communicate their work. Once we have this information, we will work with them to understand how these accounts are being used. Individual staff members must provide these details to the Security Policy mailbox by 28/02/20.

The Digital Communications team will review these accounts and work with owners to determine whether they should be operated as official Welsh Government accounts.

Where this isn't appropriate or if staff wish to retain control of the personal account on their own device, **the advice is that you remove anything that may suggest that you work for the Welsh Government**. This advice is not mandatory but not doing so by 28/02/20 means that you continue at your own risk. If you do not follow the advice and inappropriate activity is identified on your personal account (such as the example in Annex 1), you will be referred to HR for consideration of disciplinary action. As the case study shows, the targeting of individuals doesn't just happen to other people, it has happened to a colleague. Your risk profile is naturally higher if your role is in an area that is of interest to lobbyists, is high profile or senior.

LinkedIn

A key element of the social media profile on the LinkedIn platform is your current role and employer and so you may use your work email address for LinkedIn registration. A large number of staff use it to communicate their work and aid professional development. We are not suggesting that you do not use LinkedIn, however you should ensure you meet your responsibilities within the Civil Service Code.

Please be aware that the terms and conditions of LinkedIn gives the platform the right to use and reproduce any content posted. You must not post any material on LinkedIn that you would not want to see posted verbatim in the media and attributed personally to you. Remember that you must never put your security vetting status on social media.

WhatsApp

My team regularly receive requests to use WhatsApp on Welsh Government phones. A summary of our position on WhatsApp is that its use does not allow us to comply with our legal