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

responsibilities as a data controller. The full statement explains the position and includes the alternatives for staff. In the same way that personal email accounts cannot be used to undertake Welsh Government business, personal WhatsApp accounts may not be used for Welsh Government business.

Social media security
Any digital platform can be compromised, I advise that you do everything that you can to secure your personal social media accounts including LinkedIn. Annex 3 provides links to information which explains how to add two factor authentication to your personal social media accounts. These additional measures e.g. a text message being sent to your mobile phone whenever the account is accessed from a new device greatly reduce the risk of your account being compromised.

Digital Footprint
Even if you don't use social media, you have a digital footprint as others hold electronic information about you. If you are a social media user, it is worth pausing and reflecting how your social media use impacts your digital footprint. Please take time to read the guide that is published by the Centre for Protection of National Infrastructure.

Peter Kennedy
Welsh Government Senior Information Risk Owner (SIRO)

Issue date: 28 January 2020

Annex 1

Case study – Welsh Government social media incident
Note: names have been changed

A member of staff (Chris) was encouraged to use Twitter via a personal email address to promote their work. They were told that it was easier to do this than use their Welsh Government phone. Chris is highly thought of by Welsh Government colleagues and key stakeholders. Their line management had no concerns about their Twitter account.

Media organisations contacted the Press Office requiring responses because Chris' Twitter account had liked offensive material. Whilst the material was not illegal, it was incompatible with their role in Welsh Government. A key stakeholder also formally complained to Welsh Government about the matter. Whilst some were careful to state that the activity happened from Chris' account, others accused Chris directly. The First Minister also received a direct complaint.

Chris accessed their Twitter account from a personal laptop (password known to family members), a kindle (no password) and a personal mobile phone (password known to others and phone occasionally left on a desk). There was no two factor authentication on the Twitter account.

The investigation focussed on a number of possibilities:

- Chris had either deliberately or accidentally liked the content;
- A member of Chris' family had either deliberately or accidentally liked the content;
- Chris' account had been hacked.

Chris had to explain the incident to their family and directed them how to respond if approached on the phone or at home by the media. Chris realised the damage that the allegation caused to their work area and that their particular role in Welsh Government was untenable.

During the investigation, evidence was found that the account had been hacked. As evidence was found that the account had been hacked and that Chris' line management had encouraged them to use a personal Twitter account for Welsh Government use, there was no HR case to answer about Chris' social media use on this occasion.

Each case referred to HR is carefully considered on its own merits. In the specific circumstances of this case, had it not been possible to prove that Chris was not at fault, they would have faced formal disciplinary action and would not have been able to keep their current role in Welsh Government. This could have been a life changing incident for them.

Case study – Wales Office incident
In November 2019, the media reported that the UK Government in Wales Twitter account had been hacked and used to re-Tweet pornographic content.

While details of the investigation were not made public, had two factor authentication been implemented and activity restricted to devices own by the organisation, it's extremely unlikely that the incident would have occurred.

Annex 2

List of Welsh Government Social Media Accounts

The list of Welsh Government Social Media Accounts can be found at
https://documents.hf.wales.gov.uk/id:A28847595/document/versions/published

Annex 3

Two Factor Authentication (2FA) (sometimes called two-step verification)

2FA adds a layer of security to your account.

It works by requiring you to enter something that you know (your password) and something that you have e.g. a code that is sent to a pre-registered phone. We use 2FA on Welsh Government laptops – the RSA app.

Many service providers e.g. Amazon, PayPal, Twitter, Facebook, LinkedIn support the use of 2FA, but not many insist that you use it.

Some providers offer a choice of authentication methods. The more secure are those that use an authenticator app (a software token) as opposed to a text message (SMS). Free authenticator apps that are compatible with most services are the Microsoft and Google authenticator apps.

Use the https://twofactorauth.org/ website to find out if your providers e.g. email, banking, social media support 2FA. Enter the provider name in the search field e.g. Twitter to see what they support. Clicking the blue book icon on search results will take you to the provider's instruction page.

To save you looking them up, some of the common provider pages are listed below:
Google (including Gmail) - https://www.google.com/landing/2step/
Twitter - https://help.twitter.com/en/managing-your-account/two-factor-authentication
Facebook - https://www.facebook.com/help/148233965247823
Instagram - https://help.instagram.com/566810106808145
LinkedIn - https://www.linkedin.com/help/linkedin/answer/531/two-step-verification-overview?lang=en
Amazon - https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=202073820

If your account is hacked, immediately report it to the provider. Google "how to report a hacked xxxx account" to get help from the provider e.g. "how to report a hacked twitter account".