Social media: protecting what you publish

How to reduce the likelihood of unauthorised content appearing within your organisation's social media channels.

If your organisation uses social media platforms (such as Twitter, Facebook, LinkedIn or Instagram), it's important you take steps to reduce the likelihood of damaging content being posted on your behalf.

This guidance explains how you can reduce the likelihood of damaging content being posted within your own social media channel. Even if you already have an established process for posting social media content, we recommend you take a moment to review how you're using it.

This guidance is primarily for all staff responsible for setting up social media accounts. However, all staff involved in the creation, review, approval and publication of content for social media channels will also find it useful, especially those staff involved in procurement of social media tools.

In this guidance:

Social media: what is the risk?

Poorly judged content, malicious posts, or posting personal views (rather than the 'official' company line) can damage trust in organisations of all sizes. Inappropriate content within your social media channel can be at best embarrassing, and at worst cause serious reputational damage. These types of content can harm organisations both large and small, and can dramatically affect your company share prices or your reputation. They may even lead to your product or service being boycotted.

The steps outlined below can reduce risks arising from:

- attempts to spread misinformation or fake news
- hijacking for malicious purposes, such as redirecting to malicious websites
- internal staff who have a grudge posting damaging comments
- draft, incomplete or inaccurate messages being rushed into the public eye

Underlying all of these risks are a few key principles; make sure that only **authorised staff** can publish content, make sure the content is **accurate and up-to-date**, and make sure the content has gone through the necessary **authorisation** channels prior to release.

> **Note**
>
> Even if these principles are followed, social media remains a highly charged, fast moving medium, so there will always be the risk of an authorised member of staff publishing their personal views or reactions. This is why it's important:
>
> - to have emergency recovery plans in place
> - to ensure that everyone in your organisation who is involved in the production of social media is aware of the risks arising from its control, use and administration

---

Make sure that only authorised staff can publish content

Implementing a sound password policy to control access to social media accounts can help ensure that only authorised members of staff can publish content. Most social media products (including social media management tools) contain additional security features such as 2-step verification (2SV), so make sure you switch this on. Doing so will protect against attacks on those accounts that are only protected by using passwords.

There may be several people within your organisation who need access to the social media account, including the ability to publish content. In such cases:

- Ensure that account access logging (if available) is switched on. This will provide an audit trail for unauthorised posts, or anomalous access to the account.
- Use credential protection mechanisms, such as password managers.
- Make sure passwords are stored securely; do **not** store passwords in plaintext in files, or in shared, unencrypted documents on servers which can be easily accessed by unauthorised persons.
- Avoid sharing passwords, if possible. Where there's a pressing business requirement to share passwords, use additional controls to provide the required oversight. Some password managers allow users to share passwords in a more secure way (for example, they can audit access to the password and automatically sync password changes). For more information, refer to the section on **managing shared access** within the NCSC's password administration for system owners guidance.
- Using Privileged Access Management (PAM) solutions can further protect the social media accounts, as these can help to secure passwords as well as auditing user access.

Managing leavers and movers

If a member of staff with access to your social media channel leaves your organisation (or even changes roles), make sure their access to all such accounts is revoked if it's no longer required. This needs to be done promptly - ideally **before** they move - in case there's any animosity surrounding their departure or move. Doing this should form part of your organisation's wider

process to manage 'joiners, movers and leavers', which should cover managing access to all IT systems. If you're using shared passwords, changing these passwords needs to be carefully managed as part of the leavers process.

Use social media platforms (and management tools) that provide good security features

When choosing a social media platform to use, you need to consider cyber security risks involved, and the security functionality each tool provides. Such risk considerations should include:

- Does the platform support 2SV for content and account management?
- Does the platform have a password or account recovery mechanism?
- Does the platform have an incident response mechanism for notification, or reporting of issues?
- How does the platform cover legal and regulatory issues (e.g. GDPR and protecting personal data for authentication)?
- Do the providers of the platform describe how they protect data?

Social media management tools

The criteria above should also be applied to any **social media management** or **content management tools**. These are tools that work in conjunction with major social media platforms to simplify the process of scheduling, posting, and responding to content. In some cases, a single piece of content can be simultaneously published across multiple social media channels. It's therefore essential that these social media management tools are afforded **the same amount of protection as access to the social media platform itself**.

Make sure content can be reviewed and authorised before being published

With increasing pressures to create (and respond to) new material quickly, potentially damaging content can end up in your social media channel. This is more likely when you have multiple staff publishing at the same time. For this reason, it's important to implement a content workflow to manage and enforce the creation, approval, and publication of content. The exact nature of this workflow will depend on your organisation (and the objectives of your social media channel), but it should at a minimum identify the required checks and balances that each piece of content must pass before it can be published.

For example, content may need approval by a senior member of staff, a subject matter expert, or there may be specific **types** of review required (such as legal, technical or grammatical). Most social media management tools contain workflows 'out of the box', which you may have to amend to meet your own needs.

Whilst using a social media management tool won't necessarily prevent damaging content being created, it can help you to enforce workflows and formalise your review and approval process. This means you'll have more opportunities to detect and remove damaging content **before** it's posted on your 'live' social media channel. It will also reduce the likelihood of out-of-date/draft content being posted by mistake, as most content management systems (CMS's) include version control functionality (which is essential if your workflow includes multiple staff, often working remotely).

There may be times when it's tempting to bypass agreed workflows in order to respond quickly, for example during a crisis or incident. In such times, senior staff have a crucial role to play, in terms of:

- endorsing the importance of the publishing workflow, so staff are less likely to bypass the required checks and balances
- ensuring that publishing staff are all well trained on media impact
- being mindful of changes in personal circumstances that might put additional stress on staff

Use corporate devices to create and publish content

Where possible, social media staff should always use work devices to create and publish content. Staff who use their own devices may end up inadvertently posting content that's intended for their **own** channels on the **organisation's** channel, or vice versa. In addition, devices that are not managed by your organisation are harder to secure and maintain, which increases the risk of credential compromise by an attacker. It's also harder to put emergency recovery plans into action (which includes revoking access to social media tools) if you're not dealing with a managed device.

Put an emergency recovery plan in place

If an employee (or anyone else with authorised access to the account) is publishing damaging content, you'll need to make sure you're able to quickly revoke their access, most likely remotely. This will include managing access to any password vaults or password managers (where used) which contain corporate social media account access credentials.

If your social media channel is hijacked by an attacker, your priority should be regaining control of the account to contain any damage, rather than trying to correct any malicious content that's been posted. Most social media tools provide the means to verify the owner's account(s) using extra identifying information in the case of an account compromise. Make sure you know how to access this recovery information, and that it's kept up to date. If an attack has also accessed this account recovery information, then the only recourse might be to contact the social media platform owner.

Don't wait until you're in the middle of a real incident before finding what you need to do to regain control. Ensure you know in advance who to contact, and what information you'll need in order to identify yourself to the social media platform owners. For more information about how to recover accounts, refer to the relevant online support pages for your chosen platform or social media management tool.

For more general information about recovering online accounts, refer to the NCSC's guidance on recovering a hacked online account.

PUBLISHED

30 June 2020

REVIEWED

30 June 2020

VERSION

1.0

WRITTEN FOR

Self employed & sole traders

Small & medium sized organisations

Large organisations

Public sector