This template is intended as a guide for your organisation to create a suitable policy for your operations. It should always be checked to ensure that all activities or considerations are covered by this document.

The sections in **\*RED\*** are to highlight a section that can be removed or for you to edit tailored the organisation’s details. **\*INSERT ORGANISATION NAME\*** is for the name of the group / organisation. **\*INSERT ROLE\*** is for the different positions or roles within the organisation responsible for the tasks mentioned. Ensure the correct role inserted in the correct part of the policy to avoid confusion.

Always proof read the policy before signing it off! Remove this guidance once completed.

**SOCIAL MEDIA POLICY**

1. **Introduction**

Staff and Volunteers of **\*INSERT ORGANISATION NAME\*** may be able to access social media services and social networking websites at work, either through organisation IT systems or via their own personal equipment.

This social media policy describes the rules governing use of social media at **\*INSERT ORGANISATION NAME\*.**

It sets out how staff/volunteers must behave when using the organisation’s social media accounts. It also explains the rules about using personal social media accounts at work and describes what staff/volunteers should say about the organisation on their personal accounts.

This policy should be read alongside other key policies. The organisation’s internet use policy is particularly relevant to staff/volunteers using social media. **(Remove this paragraph if not relevant)**

1. **Context**

Social media can bring significant benefits to **\*INSERT ORGANISATION NAME\***, particularly for building relationships with current and potential service-users and partners.

However, it’s important that staff/volunteers who use social media within the organisation do so in a way that enhances the organisation’s connections.

A misjudged status update can generate complaints or damage the organisation’s reputation. There are also security and data protection issues to consider.

This policy explains how staff/volunteers can use social media safely and effectively.

1. **Policy scope**

This policy applies to all staff, contractors and volunteers at **\*INSERT ORGANISATION NAME\*** who use social media while delivering — no matter whether for business or personal reasons.

It applies no matter whether that social media use takes place on organisation premises, while travelling as part of the role or while working from home.

Social media sites and services include (but are not limited to):

* Popular social networks like Twitter and Facebook
* Online review websites like Reevoo and Trustpilot
* Sharing and discussion sites like Delicious and Reddit
* Photographic social networks like Flickr and Instagram
* Question and answer social networks like Quora and Yahoo Answers
* Professional social networks like LinkedIn and Sunzu
1. **Responsibilities**

Everyone who operates an organisation social media account or who uses their personal social media accounts at work has some responsibility for implementing this policy.

However, these people have key responsibilities:

The **\*INSERT ROLE\*** is ultimately responsible for ensuring that **\*INSERT ORGANISATION NAME\*** uses social media safely, appropriately and in line with the organisation’s objectives.

The organisation is responsible for providing apps and tools to manage the organisation’s social media presence and track any key performance indicators if providing IT equipment. The organisation is also responsible for proactively monitoring for social media security threats.

Staff and volunteers use their own personal devices at their own risk.

The **\*INSERT ROLE\*** is responsible for the roll out marketing ideas and campaigns through the organisation’s social media channels.

The **\*INSERT ROLE\*** is responsible for ensuring requests for assistance and support made via social media are followed up.

1. **General social media guidelines**

**The power of social media**

* 1. **\*INSERT ORGANISATION NAME\*** recognises that social media offers a platform for the organisation to perform marketing, stay connected with service users and partners and build its profile online.
	2. The organisation also believes its staff/volunteers should be involved in relevant conversations on social networks. Social media is an excellent way for staff/volunteers to make useful connections, share ideas and shape discussions.
	3. The organisation therefore encourages staff/volunteers to use social media to support the organisation’s goals and objectives.

**Basic advice**

Regardless of which social networks staff/volunteers are using, or whether they’re using business or personal accounts on organisation time, following these simple rules helps avoid the most common pitfalls:

* 1. Know the social network. Staff/volunteers should spend time becoming familiar with the social network before contributing. It’s important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates.
	2. If unsure, don’t post it. Staff/volunteers should err on the side of caution when posting to social networks. If it is felt that an update or message might cause complaints or offence, or be otherwise unsuitable, it should not be posted. Staff/volunteers can consult the **\*INSERT ROLE\*** for advice.
	3. Be thoughtful and polite. Many social media users have got into trouble simply by failing to observe basic good manners online. Staff/volunteers should adopt the same level of courtesy used when communicating via email.
	4. Look out for security threats. Staff/volunteers members should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. Further details below.
	5. Keep personal use reasonable. Although the organisation believes that having staff/volunteers who are active on social media can be valuable both to those staff/volunteers and to the business, staff should exercise restraint in how much personal use of social media they make during working hours.
	6. Don’t make promises without checking. Some social networks are very public, so staff/volunteers should not make any commitments or promises on behalf of **\*INSERT ORGANISATION NAME\*** without checking that the organisation can deliver on the promises. Direct any enquiries to the **\*INSERT ROLE\*** for further guidance.
	7. Handle complex queries via other channels. Social networks are not a good place to resolve complicated enquiries and service user or partner issues. Once a service user or partner has made contact, staff/volunteers should handle further communications via the most appropriate channel — usually email or telephone.
	8. Don’t escalate things. It’s easy to post a quick response to a contentious status update and then regret it. Staff/volunteers should always take the time to think before responding, and hold back if they are in any doubt at all.
1. **Use of organisation social media accounts**

This part of the social media policy covers all use of social media accounts owned and run by the organisation.

* 1. **Authorised users**
		1. Only people who have been authorised to use the organisation’s social networking accounts may do so.
		2. Authorisation is usually provided by the **\*INSERT ROLE\***. It is typically granted when social media-related tasks form a core part of a staff member or volunteer’s role.

Allowing only designated people to use the accounts ensures the organisation’s social media presence is consistent and cohesive.

* 1. **Creating social media accounts**
		1. New social media accounts in the organisation’s name must not be created unless approved by the **\*INSERT ROLE\***.
		2. The organisation operates its social media presence in line with a strategy that focuses on the most-appropriate social networks, given available resources.
		3. If there is a case to be made for opening a new account, staff/volunteers should raise this with the **\*INSERT ROLE\***.
	2. **Purpose of organisation social media accounts**
		1. **\*INSERT ORGANISATION NAME\***’s social media accounts may be used for many different purposes.
		2. Staff/volunteers should only post updates, messages or otherwise use these accounts when that use is clearly in line with the organisation’s overall objectives.
		3. Staff/volunteers may use organisation social media accounts to:
* Respond to service user or partner enquiries and requests for help
* Share blog posts, articles and other content created by the organisation
* Share insightful articles, videos, media and other content relevant to the cause, but created by others
* Provide supporters or followers with an insight into what goes on at the organisation
* Promote services, campaigns and events
* Support new service or event launches and other initiatives
	+ 1. Social media is a powerful tool that changes quickly. Staff/volunteers are encouraged to think of new ways to use it, and to put those ideas to the **\*INSERT ROLE\*.**
	1. **Inappropriate content and uses**
		1. **\*INSERT ORGANISATION NAME\***’s social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the organisation into disrepute.
		2. When sharing an interesting blog post, article or piece of content, staff/volunteers should always review the content thoroughly, and should not post a link based solely on a headline. Further guidelines can be found below.
1. **Use of personal social media accounts at work**

**The value of social media**

\*INSERT ORGANISATION NAME\* recognises that staff/volunteers’ personal social media accounts can generate a number of benefits. For instance:

* 1. Staff / volunteers can make relevant contacts that may be useful in their roles
	2. Staff/volunteers can discover content to help them learn and develop in their role
	3. By posting about the organisation, staff / volunteers can help to build the organisation’s profile online

As a result, the organisation is happy for staff/volunteers to spend a reasonable amount of time using their personal social media accounts at work.

**Personal social media rules**

**Acceptable use:**

* 1. Staff/volunteers may use their personal social media accounts for work-related purposes during regular hours, but must ensure this is for a specific reason (e.g. research). Social media should not affect the ability of staff/volunteers to perform their regular duties.
	2. Use of social media accounts for non-work purposes is restricted to non-work times, such as breaks and during lunch.

**Talking about the organisation:**

* 1. Staff/volunteers should ensure it is clear that their social media account does not represent **\*INSERT ORGANISATION NAME\***’s views or opinions.
	2. Staff/volunteers may wish to include a disclaimer in social media profiles: *‘The views expressed are my own and do not reflect the views of my employer.’*
1. **Safe, responsible social media use**

The rules in this section apply to:

* Any staff/volunteers using organisation social media accounts
* Staff/volunteers using personal social media accounts during organisation time

**Users must not:**

* 1. Create or transmit material that might be defamatory or incur liability for the organisation.
	2. Post message, status updates or links to material or content that is inappropriate.
	3. Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.
	4. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, gender identity, personal presentation or any other characteristic protected by law.
	5. Use social media for any illegal or criminal activities.
	6. Send offensive or harassing material to others via social media.
	7. Broadcast unsolicited views on social, political, religious or other non-business related matters.
	8. Send or post messages or material that could damage **\*INSERT ORGANISATION NAME\***’s image or reputation.
	9. Interact with **\*INSERT ORGANISATION NAME\***’s competitors in any ways which could be interpreted as being offensive, disrespectful or rude. (Communication with direct competitors should be kept to a minimum.)
	10. Discuss colleagues, competitors, customers or suppliers without their approval.
	11. Post, upload, forward or link to spam, junk email or chain emails and messages.
1. **Copyright**

**\*INSERT ORGANISATION NAME\*** respects and operates within copyright laws.

Users may not use social media to:

* 1. Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
	2. If staff/volunteers wish to share content published on another website, they are free to do so if that website has obvious sharing buttons or functions on it.
	3. Share links to illegal copies of music, films, games or other software.
1. **Security and data protection**

Staff/volunteers should be aware of the security and data protection issues that can arise from using social networks.

**Maintain confidentiality**

Users must not:

* 1. Share or link to any content or information owned by the organisation that could be considered confidential or commercially sensitive.
	2. This might include performance figures, details of service users, or information about future strategy or marketing campaigns.
	3. Share or link to any content or information owned by another organisation or person that could be considered confidential or commercially sensitive.
	4. Share or link to data in any way that could breach the organisation’s data protection policy.

**Protect social accounts**

* 1. Organisation social media accounts should be protected by strong passwords that are changed regularly and shared only with authorised users.
	2. Wherever possible, staff/volunteers should use two-factor authentication (often called mobile phone verification) to safeguard organisation accounts.
	3. Staff/volunteers must not use a new piece of software, app or service with any of the organisation’s social media accounts without receiving approval from the **\*INSERT ROLE\***

**Avoid social scams**

* 1. Staff/volunteers should watch for phishing attempts, where scammers may attempt to use deception to obtain information relating to either the organisation or its customers.
	2. Staff/volunteers should never reveal sensitive details through social media channels. Service user identities must always be verified in the usual way before any account information is shared or discussed where appropriate.
	3. Staff/volunteers should avoid clicking links in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague-sounding direct messages.
1. **Policy enforcement**

**Monitoring social media use**

* 1. Organisation IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate business use.
	2. The organisation therefore reserves the right to monitor how social networks are used and accessed through these resources.
	3. Any such examinations or monitoring will only be carried out by authorised staff.
	4. Additionally, all data relating to social networks written, sent or received through the organisation’s computer systems is part of official **\*INSERT ORGANISATION NAME\*** records.
	5. The organisation can be legally compelled to show that information to law enforcement agencies or other parties.

**Potential sanctions**

* 1. Knowingly breaching this social media policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment or involvement.
	2. Staff/volunteers, contractors and other users may also be held personally liable for violating this policy.
	3. Where appropriate, the organisation will involve the police or other law enforcement agencies in relation to breaches of this policy.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Status / Version | Date Revised | Author | Review Date | Signed By |
| 1 |  |  |  |  |