# 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version: | 1 | | | |
| Date Created: | 01st February 2024 | | | |
| Author: | Timothy Van Zyl | | | |
| Ratified by: |  | | | |
| Date Ratified: |  | | | |
| Review Date: |  | | | |
|  |  |  |  |  |
| Revision History: | | | | |
|  |  |  |  |  |
| Version | Date Created | Date Ratified | Author | Summary of Changes |
| 1.0 |  |  |  |  |
| 2.0 |  |  |  |  |
| 3.0 |  |  |  |  |
| 4.0 |  |  |  |  |
| 5.0 |  |  |  |  |

**Introduction**

Social media can bring significant benefits to Habbibi, particularly for building relationships with current and potential customers.

However, it’s important that employees who use social media within the organisation do so in a way that enhances the organisation’s prospects.

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

The Habbibi employees may be able to access social media services and social networking websites at work, either through company IT systems or via their own personal equipment.

This social media policy describes the rules governing use of social media at Habbibi.

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

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

This policy should be read alongside other key policies. The company’s Communication and Internet policy and Disciplinary policy is particularly relevant to staff using social media.

This policy applies to all Habbibi workers, full and part-time employees, agency workers, volunteers and contractors.

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy

This policy does not form part of any employee's contract of employment and it may be amended at any time

**Responsibilities**

Everyone who operates an Habbibi 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 Operations Manager is ultimately responsible for ensuring that Habbibi uses social media safely, appropriately and in line with the organisation’s objectives.
* The Chief Technical Officer is responsible for providing apps and tools to manage the organisation’s social media presence and track any key performance indicators. They are also responsible for proactively monitoring for social media security threats.
* The Operations Manager is responsible for working with our external social media company to roll out marketing ideas and campaigns through our social media channels.
* The Head Office Administrator is responsible for ensuring requests for assistance and support made via social media are followed up.

**General social media guidelines**

Habbibi recognises that social media offers a platform for the organisation to perform marketing, stay connected with customers and build its profile online.

Basic advice

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

* ***Know the social network*.** Employees 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.
* ***If unsure, don’t post it.*** Staff should err on the side of caution when posting to social networks. If an employee feels an update or message might cause complaints or offence — or be otherwise unsuitable — they should not post it. Staff members can always consult their sites General Manager for advice.
* ***Be thoughtful and polite****.* Many social media users have got into trouble simply by failing to observe basic good manners online. Employees should adopt the same level of courtesy used when communicating via email.
* ***Look out for security threats****.* Staff members should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. Further details below.
* ***Keep personal use reasonable****.* Staff should exercise restraint in how much personal use of social media they make during working hours, unless given authorisation or it forms part of their role.
* ***Don’t make promises***. Some social networks are very public, so employees should not make any commitments or promises on behalf of Habbibi, unless the organisation has authorised this in writing. Direct any enquiries to the Operations Manager.
* ***Handle complex queries via other channels.*** Social networks are not a good place to resolve complicated enquiries and customer issues. Once a customer has made contact, employees should handle further communications via the most appropriate channel — usually email or telephone.
* ***Don’t escalate things****.* It’s easy to post a quick response to a contentious status update and then regret it. Employees should always take the time to think before responding, and hold back if they are in any doubt at all.

**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.

Authorised users

Only people who have been authorised to use the organisation’s social networking accounts may do so.

Authorisation is usually provided by the Operations Manager. It is typically granted when social media-related tasks form a core part of an employee’s job.

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

Creating social media accounts

New social media accounts in the organisation’s name must not be created unless approved by the Operations Manager.

The organisation operates its social media presence in line with a strategy that focuses on the most-appropriate social networks, given available resources.

If there is a case to be made for opening a new account, employees should raise this with the Operations Manager.

Purpose of organisation social media accounts

Habbibi’s social media accounts may be used for many different purposes.

In general, employees should only post updates, messages or otherwise use these accounts when that use is clearly in line with the organisation’s overall objectives.

For instance, employees may use organisation social media accounts to:

* Respond to customer enquiries and requests for help
* Share blog posts, articles and other content created by the organisation or its external media company
* Share insightful articles, videos, media and other content relevant to the business, but created by others
* Provide fans or followers with an insight into what goes on at the organisation
* Promote marketing campaigns and special offers
* Support new product launches and other initiatives

Social media is a powerful tool that changes quickly. Employees are encouraged to think of new ways to use it, and to put those ideas to the Operations Manager.

Inappropriate content and uses

Organisation 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.

When sharing an interesting blog post, article or piece of content, employees should always review the content thoroughly, and should not post a link based solely on a headline.

Further guidelines can be found below.

**Use of personal social media accounts at work**

Habbibi recognises that employees’ personal social media accounts can generate a number of benefits. For instance:

* Staff members can make industry contacts that may be useful in their jobs
* Employees can discover content to help them learn and develop in their role

Personal social media rules

Use of social media accounts for non-work purposes is restricted to non-work times, such as breaks and during lunch. Social media should not affect the ability of employees to perform their regular duties.

Talking about the organisation:

* Employees should ensure it is clear that their social media account does not represent Habbibi’s views or opinions.
* Staff 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.’

**Safe, responsible social media use**

The rules in this section apply to:

* Any employees using organisation social media accounts
* Employees using personal social media accounts during organisation time

Users must not:

* Create or transmit material that might be defamatory or incur liability for the organisation.
* Post message, status updates or links to material or content that is inappropriate. 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. 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, or any other characteristic protected by law.
* Use social media for any illegal or criminal activities.
* Send offensive or harassing material to others via social media.
* Broadcast unsolicited views on social, political, religious or other non-business-related matters.
* Send or post messages or material that could damage Habbibi’s image, reputation or intellectual property.
* Interact with Habbibi’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.)
* Discuss colleagues, competitors, customers or suppliers without their approval.
* Post, upload, forward or link to spam, junk email or chain emails and messages.

**Copyright**

Habbibi respects and operates within copyright laws. Users may not use social media to:

* Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party and authorised by the Chief Technical Officer. If staff 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.
* Share links to illegal copies of music, films, games or other software.

**Security and data protection**

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

Maintain confidentiality

Users must not:

* Share or link to any content or information owned by the organisation that could be considered confidential or commercially sensitive. This might include food recipes, sales figures, details of key customers, or information about future strategy or marketing campaigns.
* Share or link to any content or information owned by another organisation or person that could be considered confidential or commercially sensitive. For example, if a competitor’s marketing strategy was leaked online, employees of Habbibi should not mention it on social media.
* Share or link to data in any way that could breach the organisation’s data protection policy.

Protect social accounts

* Organisation social media accounts should be protected by strong passwords that are changed regularly and shared only with authorised users.
* Wherever possible, employees should use two-factor authentication (often called mobile phone verification) to safeguard organisation accounts.
* Staff 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 Chief Technical Officer or Operations Manager.

Avoid social scams

* Staff should watch for phishing attempts, where scammers may attempt to use deception to obtain information relating to either the organisation or its customers. Employees should never reveal sensitive details through social media channels. Customer identities must always be verified in the usual way before any account information is shared or discussed.
* Employees 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.

**Policy enforcement**

Monitoring social media use

Organisation IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate business use.

The organisation therefore reserves the right to monitor how social networks are used and accessed through these resources.

Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all data relating to social networks written, sent or received through the organisation’s computer systems is part of official Habbibi records.

The organisation can be legally compelled to show that information to law enforcement agencies or other parties.

Potential sanctions

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.

Workers, full and part-time employees, agency workers, volunteers, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the organisation will involve the police or other law enforcement agencies in relation to breaches of this policy.