

Social Media Policy

Last updated: November 2023

1. Overview

Cloudoko recognises that the internet provides unique opportunities to:

- participate in interactive discussions
- engage with the wider community
- share information on particular topics

This also includes using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to the Cloudoko's reputation, confidential and proprietary information. It can also jeopardise the Cloudoko's compliance with legal obligations.

This policy aims to minimise these risks, avoid loss of productivity and ensure that Cloudoko's IT resources and communications systems are used only for appropriate business purposes. Cloudoko expects employees to adhere to this policy, which outlines staff responsibilities when accessing and using social media websites.

2. Purpose

This policy covers all individuals working at all levels including staff and volunteers (collectively referred to as staff in this policy).

This policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

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

3. Scope

This policy deals with the use of all forms of social media, which includes:

- Facebook
- LinkedIn
- Twitter
- Wikipedia
- blogs
- all other social networking sites and internet posting forums

This policy applies to the use of social media for both Cloudoko and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using Cloudoko IT facilities and equipment or equipment belonging to members of staff.

The purpose of this policy is to:

- encourage good practice
- protect the Cloudoko, its staff and clients
- clarify where and how existing policies and procedures apply to social media
- promote effective and innovative use of social media as part of Cloudoko activities

4. Policy

Protecting Cloudoko's business reputation

Staff must not post disparaging or defamatory statements about:

- Cloudoko
- its clients
- its employees

Staff should also avoid social media communications that might be misconstrued in a way that could damage Cloudoko's business reputation, even indirectly.

Unless expressly authorised to speak on behalf of the Cloudoko, either using a Cloudoko social media account or otherwise, staff should make it clear in social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal email address when communicating through social media.

Staff are personally responsible for what they communicate on social media. Staff should remember that what they publish might be available to be read by a wider audience for a long time. This audience includes the Cloudoko itself, future employers and social acquaintances. Staff should keep this in mind before posting content.

If employees disclose their position as an employee of Cloudoko, either using a Cloudoko social media account or otherwise, they must also state that their views do not represent those of their employer. This does not include staff authorised to speak on behalf of the Cloudoko. For example, employees could state, "the views in this post do not represent the views of my employer". Employees should also ensure that their profile and any content they post are consistent with the professional image they present to clients and colleagues.

Staff should avoid posting comments about sensitive business-related topics, such as Cloudoko performance. Even if staff make it clear that their views on such topics do not represent those of the Cloudoko, their comments could still damage Cloudoko's reputation or breach confidentiality obligations.

If staff are uncertain or concerned about the appropriateness of any statement or posting, they should not make any communication until discussed with their line manager.

If staff see content on social media that reflects poorly on Cloudoko or its stakeholders, they should contact their line manager. All staff are responsible for protecting Cloudoko's business reputation.

Staff should use Cloudoko email addresses for the conduct of Cloudoko business through social media. Use of private email addresses for Cloudoko business is not allowed.

Respecting intellectual property and confidential information includes the following.

1. Staff should not do anything to threaten Cloudoko's valuable trade secrets and other confidential information and intellectual property through the use of social media.
2. In addition, staff should avoid misappropriating or infringing the intellectual property of other organisations and individuals. This can create liability for Cloudoko, as well as the individual author.
3. Staff must not use Cloudoko logos, brand names, slogans or other trademarks in any social media post. This includes posting any of Cloudoko's confidential information without written consent from the <Role>.

4. To protect themselves and Cloudoko against liability for copyright infringement, where appropriate, staff should reference sources of particular information they post or upload and reference them accurately. If staff have any questions about whether a particular post or upload might violate anyone's copyright or trademark, they should seek advice from the <Role> before making the communication.

Respecting colleagues, students, clients, partners and suppliers includes the following.

1. Staff must not post anything that their colleagues, the organisation and its clients or stakeholders would find offensive. This includes discriminatory comments, insults or obscenities.
2. Staff must not post anything (comments, videos, images) related to their colleagues, or Cloudoko clients and stakeholders, without their written consent.

Responsible personnel

All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All staff are responsible for the effectiveness of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Data Protection Officer. Questions regarding the content or application of this policy should also be directed to the Data Protection Officer.

5. Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

Breach of this policy may result in disciplinary action, up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether Cloudoko equipment or facilities are used for the purpose of committing the breach.

Any member of staff suspected of committing a breach of this policy will be required to co-operate with Cloudoko's investigation. Cloudoko also reserves the right to suspend internet access where it deems it necessary during an investigation. When considering any potential breach of this policy, Cloudoko will consider the context of any social media posting.

Staff may be required to remove internet postings that are deemed to constitute a breach of this policy.

6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

The following definition and terms can be found in the Cloudoko [Glossary](#).

- Data Protection Officer

8. Revision History

Date of Change	Responsible	Summary of Change
November 2023	Kevin Boldy	Initial Version



www.cloudoko.com