



SOCIAL MEDIA POLICY

Revised and updated March 2024

Introduction

SigmaRoc is an AIM-quoted lime and limestone group targeting quarried materials assets in the UK and Northern Europe.

The SigmaRoc plc Social Media Policy is in place to minimise the risks to its business and assist employees in making appropriate decisions about the use of social media. It sets out the Company's rules and guidance in relation to employees' personal and business use of social media and social networking websites and is in addition to the Company's IT, Communication and Monitoring Policy. It outlines the circumstances in which the Company will monitor use of social media and the action which may be taken in respect of breaches of this policy.

This policy covers all employees, officers, consultants, contractors, interns, casual workers and agency workers.

Definitions

The term "social media" refers to all forms of social media and social networking websites that allow people to exchange information, ideas and opinions and to build online communities or networks. It includes but is not limited to:

- Social networking sites, such as Facebook and LinkedIn
- Investor forums, such as ADVFN
- Blogs
- Audio and video podcasts
- 'Wikis', such as Wikipedia
- Message boards
- Comments on web-articles
- Social bookmarking
- Photo, document and video sharing websites, such as Instagram and YouTube
- Miniblogs, such as Twitter.

Social media websites are fast growing and ever changing. The list above refers to some well-known examples of social media but is not exhaustive.

General Responsibilities

The Company understands and accepts that many employees engage in social networking activities. However, it is the Company's responsibility to ensure that its employees' use of social media does not damage its reputation or result in the disclosure of confidential information. The Company also has a responsibility to protect its employees from cyber-bullying (harassment caused by another employee's use of social media) and discrimination.

Employees are responsible for knowing and understanding this policy. When accessing social media websites, they must be aware that anything posted online is in the public domain and can remain so indefinitely. If the Company is identified or identifiable, any negative comments about the Company, individuals or other organisations may be attributed to the Company. As a result, the Company risks damage to its reputation and claims for liability. The Company may also be held liable for breaches of confidentiality and privacy, which are damaging to individuals and organisations.

It is the responsibility of everyone to treat others with dignity and respect. This requirement applies equally to social networking. Abusive postings about colleagues and others are likely to amount to bullying and, where they relate to a protected characteristic (age, disability, gender reassignment, marriage and civil relationship, pregnancy and maternity, race, religion or belief, sex, and sexual orientation) may also amount to discrimination, for which the Company, as well as the employee, may be held liable.

Personnel responsible for implementing the policy

The board of directors (the "**Board**") has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for its operation to the Compliance Officer. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with the Compliance Officer who will review this policy at least annually to ensure that it meets legal requirements and reflects best practice.

All staff are responsible for the success 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 Compliance Officer. Questions regarding the content or application of this policy should be directed to the Compliance Officer.

If the Board or the Compliance Officer are unsure regarding any posts they wish to publish via non-regulatory news feeds, on the Company's website or via any other form of social media, the Company shall take advice from its legal advisers and nominated adviser before approving any such public communication

Compliance and Breach of the Policy

Compliance with this policy is mandatory and forms part of the Terms and Conditions of Employment. Any use of social media, which is in breach of this policy, will be treated as misconduct and dealt with under the Company's Discipline Procedure. Serious cases will be treated as gross misconduct and may lead to dismissal. Social media should never be used in a way which breaches any of the Company's other policies.

Use of Social Media as an Employee and in an Official Capacity

Social media is a vital sales and marketing tool for the Company and the Company recognises the importance of the internet in shaping public thinking about the Company and its products. The Company also recognises the importance of its employees joining in and helping shape industry conversation and direction through interaction in social media.

Before using work-related social media employees must have read and understood this policy.

Only employees who have been given express permission are permitted to access and post material on a social media website in the Company's name and on its behalf. There must be a genuine business case for such access and posting and the employee must have obtained prior authorisation from their manager.

Personal Use of Social Media at work

The Company allows employees to use its computer facilities to access social networking websites for personal use provided that such use is limited to before and after normal working hours and during official breaks. The Company retains the absolute right at any time to withdraw its permission for employees to use its facilities to access social media and/or to block access to any social media website.

Employees may use their own computer facilities to access social networking sites while they are at work but only during their non-working hours, that is, before and after normal working hours and during official breaks.

All employees who access social networking websites, whether using the Company's or their own facilities, must comply with the rules as set out in this policy.

Use of Social Media outside Work

The Company acknowledges the popularity of social media and the right that employees have to engage in social networking activities outside work. However, in order to fulfil its own responsibilities for protecting its reputation, its employees and confidential information, the Company requires employees to comply with the rules as set out in this policy.

Rules Governing All Use of Social Media

When using social media and social networking sites, employees are required to comply with the following rules.

Employees must not:

- Identify themselves as working for the Company or use the Company's logo, unless authorised to do so by a Director
- Express opinions on behalf of the Company, subject to paragraph 5 above
- Express personal views about the Company, its employees, its clients or any other individual or organisation that could be seen as offensive or defamatory
- Comment on the Company's position on any issue (including but not limited to its strategies, policies, plans, processes, history, appointments, finances, acquisitions, recruitment, pay and benefits)
- Disclose commercially sensitive, private or confidential information including but not limited to personal information about individuals, client details, financial and commercially sensitive information about the Company or its clients, future business plans, trade secrets and intellectual property. Confidential information can include photos and videos. Employees are required to comply with the Company's Data Protection Policy in relation to all confidential information, which may include but is not limited to those items described above.
- Breach copyright by using (or otherwise upload, post or forward) intellectual property (text or images) or other content belonging to another person or organisation without their consent or and/or without acknowledgement
- Post any text or image in relation to any other individual that could be perceived as abusive, obscene, discriminatory, bullying, harassing, derogatory or victimising.

- Make false or misleading statements or impersonate colleagues or third parties
- Provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the Company. Therefore the Company does not permit the use of LinkedIn recommendations for employees
- Generally damage the Company's business interests or reputation, even indirectly, including making any comments that could reasonably be expected to embarrass or compromise the Company or any of its stakeholders

Employees must:

- Take all necessary steps to avoid identity theft, for example by not revealing personal and contact details including their address, bank details or passport number or those of any other third party
- Make it clear in social media postings, or on their personal profile, that they are speaking on their own behalf. Write in the first person and use a personal e-mail address
- If disclosing their affiliation with the Company on their profile or in any social media postings, state that their views do not represent those of the Company, unless authorised to speak on the Company's behalf as set out in paragraph 5 above
- Be personally responsible for content published on social media tools and be aware that what is published will be public for many years
- Contact their manager or a member of the Board if they see social media content that disparages or reflects poorly on the Company or any of its stakeholders
- Alert their manager if they become aware of any breach of this policy.

Listed Company - Social Media and Price Sensitive Information

All employees must be conscious that they work within a company which is quoted on the AIM market of the London Stock Exchange plc and, as a result, they may become aware of information which may be "price sensitive", that is, information which, if made public, would be likely to have a significant effect on the price of shares in the Company. The AIM Rules for Companies ("**AIM Rules**") provide that a company must make an announcement to the public via an approved Regulatory Information Service ("**RIS**") without delay of any developments which are not public knowledge and which may be "price sensitive". This may include matters concerning a change in the company's financial condition, sphere of activity, performance of business or its expectation of its performance.

Where the Company is required to make a RIS notification, the notification must be made no later than the information is published elsewhere. The fact that information released through other outlets is or may become publicly available is not a substitute for making a notification under the AIM Rules. Consequently, the requirement to make a notification under the AIM Rules will not be satisfied by disclosure via social media and the Company must, in each case, make an RIS announcement.

All regulatory information must be disclosed to the market in a fair and timely manner and the formal channels of disclosure must be adhered to. A company's securities can be suspended from trading where there has been an unusual share price movement because of an inequality of information provided to the market. The London Stock Exchange plc can investigate and take such disciplinary action as it considers appropriate in such an instance.

It is also an offence under the retained EU law version of the Market Abuse Regulation (596/2014) and relevant technical standards relating thereto as they form part of United Kingdom domestic law by virtue of the European Union (Withdrawal) Act 2018 ("UK MAR") to unlawfully disclose such information, and premature or selective disclosures or disclosures designed to cause volatility in the Company's share price (e.g. a leak of confidential information), which may constitute market abuse under UK MAR, falling under the regulation of the Financial

Conduct Authority, who may impose penalties (including unlimited fines) on both the Company and its directors for market abuse.

This policy prohibits the disclosure of price sensitive information on social media. Disclosure of price sensitive information may also constitute a criminal offence. If anyone has any queries whether information they are aware of may, or may not be, "price sensitive" they should discuss this with a Director.

Monitoring the use of Company Facilities

The Company reserves the right to monitor employees' use of its facilities to access social media and social networking websites.