ROCKFIRE RESOURCES PLC SOCIAL MEDIA POLICY

This Social Media Policy does not form part of your contract of employment and where Rockfire plc (the "Company") considers appropriate, it may amend the policy from time to time or depart from it or adjust how it is applied.

1. About this Policy

1.1 This Policy is in place to minimise the risks to the Company's business through use of social media. This Policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers and agency workers.

1.2 This Policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, Instagram and all other social networking sites, internet postings and blogs.

2. Using Social Media

2.1 Social networking in every form provides the Company with a tremendous opportunity to spread the good word about what it does, what its clients and partners are doing and the Company's work.

2.2 However, employees' use of social media can pose risks to the Company's confidential information and reputation, and can jeopardise its compliance with legal and regulatory obligations.

2.3 Online social networks blur the lines between public and private information. By virtue of you identifying yourself as an employee of the Company within a social network, you should ensure that content associated with you is consistent with your work and the Company's brand. This Policy applies to use of social media for business purposes as well as personal use that may affect the Company's business in any way. If you are in any doubt on whether you need authorisation to post an item on social media, or whether a post will breach this Policy, you should check with the CEO.

3. Compliance with Related Policies and Prohibited Use

3.1 Social media should never be used in a way that breaches any of the Company's other policies. If an internet post would breach any of the Company's policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to:

(a) breach the Company's Code of Conduct;

(b) breach any obligations contained in those policies relating to confidentiality;

(c) breach any other laws or regulatory requirements.

3.2 The same principles and guidelines that apply to the Company's activities in general apply to all online activities. This includes all forms of online publishing and discussion (whether for personal use or on behalf of the Company) including blogs, wikis, user-generated video and audio, virtual worlds and social networks.

3.3 You should never provide references for other individuals on social or professional networking sites, as such references (whether positive or negative) can be attributed to the Company and can create legal liability for both the author of the reference and the Company.

3.4 You must avoid making any social media communications that could damage the Company's business interests or reputation, even indirectly.

3.5 You must not use social media to:

(a) defame or disparage the Company, its staff or any third party;

(b) harass, bully or unlawfully discriminate against staff or third parties;

(c) make false or misleading statements; or

(d) impersonate colleagues or third parties.

3.6 You must not post comments about sensitive business-related topics, such as the Company's performance, or do anything to jeopardise the Company's trade secrets, confidential information or intellectual property.

3.7 You must not make any reference, directly or indirectly, to business-related topics that are in the course of negotiation, such as potential contracts.

3.8 You must also be conscious that you work within a group of companies which is listed on the AIM and that, as a result, we 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. Our policy prohibits the disclosure of price sensitive information on social media. Disclosure of price sensitive information may also constitute a criminal offence.

3.9 The contact details of business contacts made during the course of your employment or engagement with the Company are the Company's confidential information. On termination of your contract with the Company, you must provide the Company with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.

3.10 Any employees that act in breach of any of the above (whether whilst posting in a personal capacity or on behalf of the Company) may be subject to disciplinary action up to and including the termination of their employment and any other staff or contractors that do likewise may have their contracts terminated immediately.

4. Personal use of social media

4.1 In general, what you do in your own time is your business. However, activities in or outside of work that adversely affect: (1) your job performance; (2) the performance of others; or (3) the Company's legitimate business interests, are a proper focus for this Policy.

4.2 You should be respectful to others when making any statement on social media and be aware that you will be personally responsible for all communications published on the internet for anyone to see.

4.3 You must not express opinions on the Company's behalf or include the Company's logos or other trademarks via social media, unless expressly authorised to do so by the CEO. You may be required to undergo training in order to obtain such authorisation.

4.4 If you do disclose your affiliation with the Company on your profile or in any social media postings, you should make it clear in the social media post, or in your personal profile, that you are speaking on your own behalf. You should write in the first person and use a personal e-mail address. You must:

(a) state that your views do not represent those of the Company. For instance, in a personal blog, the following standard disclaimer should be prominently displayed: *"The postings on this site are my own and don't represent my employer's opinions."*;

(b) act in accordance with the guidelines in this Policy; and

(c) seek prior approval from the CEO if you are unsure whether what you are intending to post is appropriate.

4.5 You should always remember that personal posts, even if sent outside of work hours or premises and regardless of whether the social media is accessed using the Company's IT and communications facilities and equipment, may still defame or disparage the Company (or its staff or any third party), either directly or by way of association and may lead to disciplinary action being taken against employees up to and including dismissal or contracts of contractors being terminated.

5. Business use of social media by employees

5.1 You may only speak or post on behalf of the Company in a social media environment when specifically authorised to do so by the Company.

5.2 If you are required for business purposes to speak on behalf of the Company in a social media environment, you must still seek prior approval for such communication from the CEO and must act in accordance with the guidelines in this Policy.

5.3 Care must be taken to ensure that any social media posts do not contain any sensitive information related to the Company or any of its clients.

5.4 Any proposed posts which [could be considered to contain sensitive information/make reference to the business performance of the Company, its contracts or any of its clients] must be approved in advanced by the CEO.

5.5 In general, reposting of news which has already been notified by the Company under RNS or an equivalent regulatory information service is permitted.

5.6 You must not misuse the Company's logos or trademarks and must only use them if you have the authority to do so. For example, you should not use "Rockfire Resources PLC" in your screen name or other social media ID.

6. Use of social media by Directors and persons discharging managerial responsibilities (PDMRs)

6.1 Directors and PDMRs who have access to inside information must be mindful of the Company's obligations under the Market Abuse Regime (MAR) and the AIM Rules for Companies.

6.2 You must not use social media to disseminate information which could constitute inside information as defined under Article 19 of MAR.

6.3 Yellow Jersey will monitor posts by Directors and PDMRs related to the Company. e.g., require prior approval by another board member of the Chairman/restrict any posts to reposts/links to RNS announcements once they have been released.

7. Business use of social media on behalf of the Company by third parties

7.1 No third party may be engaged to undertake social media activities on behalf of the Company without the prior approval of [the Board].

8. Monitoring

8.1 The Company reserves the right to monitor, intercept and review, without further notice, your online social media postings and activities related to the Company, to ensure that the Company's rules are being adhered to and for legitimate business purposes and you consent to such monitoring.

9. Recruitment

9.1 The Company may use internet searches to perform due diligence on candidates in the course of recruitment.

10. Breaches

10.1 Any breach of this Policy by employees may result in disciplinary action up to and including their dismissal, and any other member of staff or contractor may have their contracts terminated immediately where such a breach has occurred. If you are suspected of committing a breach of this Policy you will be required to co-operate with the Company's investigation, which may involve handing over relevant passwords and login details.

10.2 You may be required to remove any social media content that the Company considers a breach of this Policy. Failure to comply with such a request may in itself result in disciplinary action being taken or contracts being terminated.

This policy was last updated on 2 March 2022

Reviewed by Gordon Hart
Chairman Rockfire Resources plc