

GENinCode PLC (the Company)

Social Media Policy

Dated: 23 June 2021



Version: 1.0

23 Jun 2021

1. ABOUT THIS POLICY

- 1.1 This policy:
- 1.2 covers all individuals working at all levels and grades, including senior managers, directors, employees, officers, consultants, contractors, homeworkers, part-time and fixed-term employees, casual colleagues, agency colleagues and volunteers (collectively referred to as **colleagues** in this policy);
- 1.3 deals with the use of all forms of social media and instant messaging systems, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Instagram, TikTok, WhatsApp, iMessage, Facebook Messenger, Line, Signal, Skype, Snapchat, and all other social networking sites, internet postings and blogs;
- 1.4 applies to all colleagues and sets out the rules both in relation to the Company's social media accounts (if any) and personal social media usage by colleagues.
- 1.5 applies to the use of social media for both business and personal purposes, whether or not during office hours or otherwise;
- 1.6 applies regardless of whether or not the social media is accessed using the Company's IT facilities and equipment or equipment belonging to colleagues; and
- 1.7 does not form part of any contract of employment and the Company may amend it at any time.

2. PEOPLE RESPONSIBLE FOR THIS POLICY

- 2.1 Everyone has a responsibility for reading and implementing this policy. The Chief Executive Officer has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Head of UK Business Development.
- 2.2 Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with the Chief Executive Officer who will review this policy annually to ensure that it meets legal requirements and reflects best practice.
- 2.3 Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all colleagues understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.
- 2.4 All colleagues 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 relevant Head of Department in the first instance. Questions regarding the content or application of this policy should be directed to the Head of UK Business Development.

3. HOW THIS POLICY IS RELATED TO OUR OTHER POLICIES

3.1 Social media should never be used in a way that breaches any of our 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, colleagues are prohibited from using social media to:

- (a) breach the Company's Employee Handbook;
- (b) breach the Company's IT policy;
- (c) breach any obligations relating to confidentiality;
- (d) defame or disparage the organisation or its affiliates, customers, clients, business partners, competitors, suppliers, vendors or other stakeholders;
- (e) unlawfully discriminate against other colleagues or third parties;
- (f) breach the Company's Data Protection Policy (for example, never disclose personal information about a colleague or third party online); and
- (g) breach any other laws, regulatory requirements or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements),

or such other similar policies as the Company may enact from time to time.

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

3.4 Colleagues who breach any of the above policies may be subject to disciplinary action up to and including termination of employment.

3.5 The Company is required under the retained UK law version of the Market Abuse Regulation (Regulation 596/2014/EU) pursuant to the European Union (Withdrawal) Act 2018, as amended, and the AIM Rules to announce to the stock market certain important information ("**Regulatory Information**"). Regulatory Information includes:

- (a) information that could affect the Company's share price - e.g. financial results; details of significant acquisitions and disposals; a material change

to or termination of a major contract; or key developments in actual or threatened legal or regulatory proceedings;

- (b) information relating to the appointment or departure of a director; and
- (c) information relating to changes in the Company' significant shareholders.

3.6 Regulatory Information must be announced via a Regulatory Information Service ("RIS") before, or at least no later than, it is made public via social media or any other means. It is permissible also to release Regulatory Information via social media either at the same time as or after an RIS announcement has been made, but releasing Regulatory Information via social media is not a substitute for announcing it via an RIS.

3.7 The requirement to announce Regulatory Information via an RIS is designed to ensure that all investors have the opportunity to receive such information simultaneously via a single specified channel. The London Stock Exchange and the Financial Conduct Authority take breaches of the requirement very seriously. They will investigate any suspected breach and can impose a variety of sanctions: these include suspending the Company's shares from trading until an adequate RIS announcement is made, and imposing fines on both the Company and its directors. In addition, where comments made on behalf of the Company via social media are inconsistent with an announcement made via an RIS, the Company may have to make a clarificatory RIS announcement.

3.8 If you yourself are proposing to release information via social media that may include Regulatory Information, or if you are unclear as to whether such information constitutes Regulatory Information, or you are proposing to arrange for a third party to do so, you must first consult the Chief Financial Officer by e-mail at pfoulger@genincode.com or the Chief Executive Officer of the Company.

4. PERSONAL USE OF SOCIAL MEDIA

4.1 Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with the individual's employment responsibilities or productivity and complies with this policy.

5. PROHIBITED USE

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

5.2 Colleagues must not use social media to defame or disparage the Company, the Company's colleagues or any third party; to harass, bully or unlawfully discriminate against colleagues or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

- 5.3 Colleagues must not express opinions on the Company's behalf via social media, unless expressly authorised to do so by their manager. Colleagues may be required to undergo training in order to obtain such authorisation.
- 5.4 Colleagues must not post comments about sensitive business-related topics, such as the Company's financial performance, or do anything to jeopardise the Company's trade secrets, confidential information and intellectual property. Colleagues must not include the Company's logos or other trademarks in any social media posting or in their profile on any social media.
- 5.5 Colleagues must not post, access, view, download, print or store any pornographic material or material of a sexually explicit nature or material that may be deemed offensive or obscene by another person.
- 5.6 Colleagues must not commit the Company to any form of contract through social media websites.
- 5.7 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.

6. USING SOCIAL MEDIA FOR BUSINESS

- 6.1 If a colleague's duties require them to speak on behalf of the organisation in a social media environment, they must still seek approval for such communication from their manager, who may require them to undergo training before they do so and impose certain requirements and restrictions with regard to their activities.
- 6.2 Likewise, if a colleague is contacted for comments about the organisation for publication anywhere, including in any social media outlet, they must direct the enquiry to the Head of PR and not respond without written approval.
- 6.3 The use of social media for business purposes is subject to the remainder of this policy.

7. GUIDELINES

- 7.1 The following sections of the policy provide colleagues with common-sense guidelines and recommendations for using social media responsibly and safely.
- 7.2 Respecting intellectual property and confidential information:
 - (a) Colleagues should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for the organisation, as well as the individual author.

- (b) To protect themselves and the organisation against liability for copyright infringement, where appropriate, colleagues should reference sources of particular information posted or uploaded and cite them accurately. If colleagues have any questions about whether a particular post or upload might infringe anyone's copyright or trademark, they should ask the marketing department before making the communication.

7.3 Respecting colleagues, clients, partners and suppliers:

- (a) Colleagues should not post anything that their colleagues or the Company's customers, clients, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.
- (b) Colleagues should not post anything related to their colleagues or the Company's customers, clients, business partners, suppliers, vendors or other stakeholders without their written permission.

7.4 Colleagues should make it clear in social media postings, or in their personal profile, that they are speaking on their own behalf, write in the first person and use a personal email address.

7.5 Colleagues should be respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for anyone to see.

7.6 If colleagues disclose their affiliation with the Company on their profile or in any social media postings, they must state that their views do not represent those of their employer (unless they are authorised to speak on the Company's behalf as set out in paragraph 5.3). Colleagues should also ensure that their profile and any content they post are consistent with the professional image they present to clients and colleagues.

7.7 If colleagues are uncertain or concerned about the appropriateness of any statement or posting, they should refrain from posting it until they have discussed it with their manager.

7.8 If colleagues see social media content that disparages or reflects poorly on the Company, they should contact their manager and/or the HR department.

8. **MONITORING**

8.1 The Company reserves the right to monitor, intercept and review, without further notice, colleagues activities using the Company's IT resources and communications systems, including but not limited to social media postings and activities, to ensure that the Company's rules are being complied with and for legitimate business purposes. By using such resources and systems colleagues consent to such monitoring.

8.2 For further information, please refer to the Company's IT Acceptable Use Policy.

9. RECRUITMENT

The Company may use internet searches to perform due diligence on candidates in the course of recruitment. Where the Company does this, it will act in accordance with its data protection and equal opportunities obligations. However, you must not use social media to undertake due diligence of potential candidates from your personal account and must obtain your manager's permission if you are asked to do so from a business account.

10. BREACH OF THIS POLICY

10.1 Breach of this policy may result in disciplinary action up to and including dismissal. Any colleague suspected of committing a breach of this policy will be required to cooperate with the Company's investigation, which may involve handing over relevant passwords and login details.

10.2 Colleagues may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.