Armadillo Lighting
Bigods Hall | Bigods Lane
Great Dunmow | Essex CM6 3BE

Armadillo Marketing Limited Social Media Policy

1. Purpose

We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to our confidential and proprietary information, and reputation, and can jeopardise our compliance with legal obligations.

To minimise these risks, to avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate business purposes, we expect employees to adhere to this policy.

2. Scope

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

2.1 It applies to the use of social media for both business and personal purposes, whether during office hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

2.2 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 our 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 our investigation, which may involve handing over relevant passwords and login details.

2.3 Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

3. Legal and Policy Framework

3.1 Employees are bound by all current UK and International law, standards and guidelines. Including but not limited to:

- The Data Protection Act (1998)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- Police & Criminal Evidence Act (amended 2008)
- The Health & Safety at Work Act (1974)
- Human Rights Act (1998)

3.2 This Policy must be read in conjunction with the following policy

- Electronic Information and Communications Policy
- Confidentiality Policy
- Data Protection Policy

4. Responsibilites

4.1 Our board of directors (the board) has overall responsibility for the effective operation of this policy.

4.2 Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Technical Director.

4.3 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.

4.4 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 Technical Department. Questions regarding the content or application of this policy should be directed to the Technical Director.

5. Policy

5.1 **Compliance with related policies and agreements**

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

- breach our Electronic Information and Communications Systems Policy;
- breach our obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations they may have relating to confidentiality;
- breach our Disciplinary Rules;
- defame or disparage the organisation or its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;
- harass or bully other staff in any way or breach our Anti-harassment and Bullying Policy;
- unlawfully discriminate against other staff or third parties or breach our Equal Opportunities Policy;
- breach our Data Protection Policy (for example, never disclose personal information about a colleague online);
- breach any other laws 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).

5.2 Staff 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.

5.3 Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

5.4 Personal use of social media

We recognise that employees may work long hours and occasionally may desire to use social media for personal activities at the office or by means of our computers, networks and other IT resources and communications systems. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the organisation's business are also prohibited.

5.5 Monitoring

The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

5.6 We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by [your acknowledgement of this policy and] your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

5.7 We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

5.8 Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

5.9 For further information, please refer to our Electronic Information and Communications Systems Policy.

5.10 Business use of social media

If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from your manager , who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

5.11 Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the inquiry to Managing Director and do not respond without written approval.

5.12 The use of social media for business purposes is subject to the remainder of this policy.

5.13 Recruitment

We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

5.14 Responsible use of social media

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

5.15 Protecting our business reputation:

a) Staff must not post disparaging or defamatory statements about:

- our organisation;
- our clients;
- suppliers and vendors; and
- other affiliates and stakeholders,

but staff should also avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.

b) Staff should make it clear in social media postings that they are speaking on their own behalf. Write in the first person and use a personal e-mail address when communicating via social media.

c) Staff are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by the masses (including the organisation itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

d) If you disclose your affiliation as an employee of our organisation, you must also state that your views do not represent those of your employer. For example, you could state, "the views in this posting do not represent the views of my employer". You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

e) Avoid posting comments about sensitive business-related topics, such as our performance. Even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation.

f) If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with your manager .

g) If you see content in social media that disparages or reflects poorly on our organisation or our stakeholders, you should contact your manager. All staff are responsible for protecting our business reputation.

5.16 **Respecting intellectual property and confidential information:**

a) Staff should not do anything to jeopardise our valuable trade secrets and other confidential information and intellectual property through the use of social media.

b) In addition, staff 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.

c) Do not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.

d) To protect yourself and the organisation against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Managing Director before making the communication.

e) The contact details of business contacts made during the course of your employment are regarded as our confidential information, and as such you will be required to delete all such details from your personal social networking accounts, such as Facebook accounts or LinkedIn accounts, on termination of employment.

5.17 **Respecting colleagues, clients, partners and suppliers:**

a) Do not post anything that your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.

b) Do not post anything related to your colleagues or our customers, clients, business partners, suppliers, vendors or other stakeholders without their written permission.