

Live Active Leisure

SOCIAL MEDIA POLICY

INTRODUCTION

Live Active Leisure [the Company] recognises that the internet provides unique opportunities to participate in interactive discussions and to share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, **Our People's** use of social media can pose risks to the Company's confidential and proprietary information, and reputation, and can jeopardise its compliance with legal obligations. To minimise these risks, to avoid loss of productivity and to ensure that the Company's IT resources and communications systems are used only for appropriate business purposes, we expect **Our People** to adhere to this policy.

SCOPE

This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, relief and agency staff and volunteers (collectively referred to as **Employees** in this policy). Third parties who have access to the Company's electronic communication systems and equipment are also required to comply with this policy.

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.

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 the Company's IT facilities and equipment or equipment belonging to individual Employees.

RESPONSIBILITY FOR COMPLIANCE WITH POLICY

All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that Employees understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements. Managers will be given training in order to do this.

Employees 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 HR & Admin Manager. Questions regarding the content or application of this policy should be directed to HR & Admin Manager.

THE POLICY IN OPERATION

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 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 the Company's IT & Communications policy
- breach the Company's obligations with respect to the rules of relevant regulatory bodies
- breach any obligations they may have relating to confidentiality
- breach the Company's Disciplinary Policy

- defame or disparage the organisation or its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders
- harass or bully other Employees in any way or breach the Company's Anti-harassment and bullying policy
- unlawfully discriminate against other Employees or third parties or breach the Company's Equality & Diversity policy
- breach the Company's 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)

Employees 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.

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

PERSONAL USE OF SOCIAL MEDIA

Personal use of social media is never permitted during working time or by means of the Company's computers, networks and other IT resources and communications systems. However the Company recognises that employees may work long hours and occasionally during authorised breaks may desire to use social media for personal activities at the office or by means of the Company's computers, networks and other IT resources and communications systems. The Company 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.

BUSINESS USE OF SOCIAL MEDIA

If an Employee's duties requires them to speak on behalf of the organisation in a social media environment, the Employee must still seek approval for such communication from Senior Management Team, who may require the Employee to undergo training before they do so and impose certain requirements and restrictions with regard to their activities.

Likewise, if Employees are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the inquiry to Senior Management Team and do not respond without written approval.

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

OUR PEOPLE and SOCIAL MEDIA COMMUNICATION

The Company will use social media such as Facebook and Twitter, to communicate to **Our People**, which will encourage on occasions two way communications when sharing and discussing information.

Our People engaging in this communication should be mindful of the Social Media policy and adhere to the key principles and tips as noted below;

Key principles and tips!

Use your best judgment. Remember to always use good judgment and common sense in deciding what you publish. If you're about to post something that makes you even the slightest bit uncomfortable, don't! Ultimately, however, you have sole responsibility for what you post in any form of online social media.

Don't forget your day job. You should make sure that your online activities do not interfere with performing your job responsibilities or commitments to customers.

Spirited and passionate discussions and debates are fine, but you should be respectful of others and their opinions. Be the first to correct your own mistakes.

Try to add value. Provide worthwhile information and perspective for your colleagues to respond to.

It is very much in the Company's interest and, we believe, **Our People** to be aware of and participate in this sphere of information, interaction and idea exchange for two reasons:

To learn: We believe in the importance of open exchange-between **Our People** — for learning. Social media can be significant for organisational and individual development.

To contribute: **Our People** make important daily contributions to the Company's success and to future business, it is important to share the exciting things we're learning and doing. Our Company's Information Technology Policy and other policies still apply. You are responsible for your actions. We encourage you to get online and have fun, but use sound judgment and common sense.

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.

RESPONSIBLE USE OF SOCIAL MEDIA

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

Employees must not post disparaging or defamatory statements about:

- the Company's organisation
- clients
- suppliers and vendors and
- other affiliates and stakeholders

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

Employees 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.

Employees are personally responsible for what they communicate in social media. Employees should remember that what they publish might be available to be read by the masses (including the organisation

itself, future employers and social acquaintances) for a long time. This should be kept in mind before any content is posted.

If Employees disclose their affiliation as an employee of the Company's organisation, they must also state that their views do not represent those of the Company. For example, Employees could state, "the views in this posting 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.

Avoid posting comments about sensitive business-related topics, such as the Company's performance. Even if Employees make it clear that their views on such topics do not represent those of the organisation, their comments could still damage the Company's reputation.

If an Employee is uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they have discussed it with a member of the Senior Management Team.

If an Employee sees content in social media that disparages or reflects poorly on the Company or its stakeholders, they should contact the Senior Management Team. Employees are responsible for protecting the Company's business reputation.

RESPECTING INTELLECTUAL PROPERTY AND CONFIDENTIAL INFORMATION

Employees should not do anything to jeopardise the Company's valuable trade secrets and other confidential information and intellectual property through the use of social media. In addition, Employees 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.

Employees are not permitted to use the Company's logos, brand names, slogans or other trademarks, or post any of the Company's confidential or proprietary information without prior written permission.

The contact details of business contacts made during the course of the Employee's employment are regarded as the Company's confidential information, and as such the Employee will be required to delete all such details from their personal social networking accounts, such as Facebook accounts or LinkedIn accounts, on termination of employment.

RESPECTING COLLEAGUES, CLIENTS, PARTNERS AND SUPPLIERS

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

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

MONITORING

The contents of the Company's IT resources and communications systems are the Company's property. Therefore, Employees 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.

The Company reserves the right to monitor, intercept and review, without further notice, Employee 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 and the Employee consents to such monitoring by their acknowledgement of this policy and their 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.

The Company 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.

Employees should not use the Company's IT resources and communications systems for any matter that you wish to be kept private or confidential from the organisation.

FAILURE TO COMPLY WITH POLICY

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 Employee 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.

Employees 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.