SOCIAL MEDIA POLICY

Policy Owner	Andrew Martin
Policy Sponsor	Andrew Martin

Version Control	Date of Review	Date of Next Review	Reviewed by
V1	24/08/2021	24/08/2024	SHSE

CORPORATE FIT	
Internal Management Plan	✓
Risk Register	✓
Business Plan	
Regulatory Standards	✓
Equalities Strategy	
Legislation	

CONTENTS

1. Introduction and Policy Statement

Part of our key aims of The Albyn Group is to build our Purpose, our Mission, our Values and our Vision into our policy and decision making on a daily basis. With that in mind, we aim to follow our guiding principles that apply to all policies: https://www.albynhousing.org.uk/about-us/.

The Group 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, Snapchat, Instagram, blogs and wikis. However, employees' use of social media can pose risks to the Group'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 Group's IT resources and communications systems are used only for appropriate business purposes, we expect employees to adhere to this policy.

2. Scope

This policy covers all individuals working at all levels and grades, including senior managers, officers, directors, Board members, employees, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers within the Group ("**Employees**"). Third parties who have access to the Group'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, Instagram, Tumblr, 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 Group's IT facilities and equipment or equipment belonging to individual Employees.

3. 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.

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 by Employees should be reported to the Head of HR. Where it relates to a Board

member, this should be reported to the Chief Executive. Questions regarding the content or application of this policy should be directed to the Head of HR.

The Policy in Operation

Social media should never be used in a way that breaches any of the Group'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 Group's ICT policies (for example, the ICT Acceptable Usage Policy);
- breach the Group's obligations with respect to the rules of relevant regulatory bodies;
- breach any obligations they may have relating to confidentiality;
- breach the Group's Disciplinary Policy;
- breach the AHS Employee or GBM Code of Conduct;
- defame or disparage the Group or its affiliates, tenants, customers, clients, business partners, suppliers, vendors or other stakeholders;
- harass or bully other Employees in any way or breach the Group's Harassment and Bullying policy;
- unlawfully discriminate against other Employees or third parties or breach the Group's Equal Opportunities policy;
- breach the Group'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 Group and create legal liability for both the author of the reference and the Group.

Examples of scenarios that are not acceptable:

- Endorsing a Group contractor's skills on LinkedIn.
- Posting about poor workmanship from a Group contractor on Facebook.

Examples of scenarios that are acceptable:

- Following a Group contractor's page on Facebook.
- Liking a Group contractor's post on LinkedIn.
- Leaving a general comment on a Group contractor's post on LinkedIn.

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

4. Personal Use of Social Media

Personal use of social media is set out in the ICT Acceptable Usage Policy, section: 3.7.4 Electronic Communication - Blogging, Community Sites and Social Networking. It is also set out in the AHS Employee Code of Conduct, section: B. Openness and Accountability, Using Social Media B.10.

The expectation of Board member's use of social media is set out in the GBM Code of Conduct.

5. Business Use of Social Media

If an Employee's duties require them to speak on behalf of the Group in a social media environment, the Employee must still seek approval for such communication from the Social Media & Communications Officer, 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 Group for publication anywhere, including in any social media outlet, direct the inquiry to the Social Media & Communications Officer and do not respond without written approval.

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

6. 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.

7. 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 Group;
- tenants and 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 Group 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 Group, they must also state that their views do not represent those of the Group. 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 tenants, clients and colleagues.

Avoid posting comments about sensitive business-related topics, such as the Group's performance. Even if Employees make it clear that their views on such topics do not represent those of the Group, their comments could still damage the Group'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 their manager or the Social Media & Communications Officer.

If an Employee sees content in social media that disparages or reflects poorly on the Group or its stakeholders, they should contact the Social Media & Communications Officer and appropriate operational manager or leadership team member. Employees are responsible for protecting the Group's business reputation.

8. Respecting Intellectual Property and Confidential Information

Employees should not do anything to jeopardise the Group's 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 without express permission, which can create liability for the Group, as well as the individual author.

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

To protect themselves and the Group against liability for copyright infringement, where appropriate, Employees should reference sources of particular information they post or upload and cite them accurately. If an Employee has any questions about whether a particular post or upload might violate anyone's copyright or trademark, they should ask the Social Media & Communications Officer before making the communication.

For professional purposes, employees are permitted to add business contacts made during the course of their employment to business networking sites, such as LinkedIn.

9. Respecting Colleagues, Tenants, Clients, Partners and Suppliers

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

10. Monitoring

Monitoring of the Group's IT resources and communications systems are set out in the ICT Acceptable Usage Policy, ICT Security Policy, and Workplace Monitoring Policy (as applicable). Employees should not use the Group's IT resources and communications systems for any matter that you wish to be kept private or confidential from the Group.

11. Failure to Comply with Policy

Breach of this policy may result in disciplinary action up to and including dismissal for senior managers, officers, directors, employees, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers. For Board members, 'Protocol for Dealing with the Code of Conduct' will be followed. 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 any subsequent 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.