



SOCIAL MEDIA POLICY

NWH Group Limited
Reviewed- January 2026

1. Policy Statement

We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can threaten our confidential and proprietary information and reputation and jeopardise our compliance with legal obligations such as GDPR (General Data Protection Regulations).

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

A misjudged status update or comment can generate complaints, damage the business's reputation, or offend others. It can also breach employee or customer confidentiality.

This policy may be amended at any time.

2. Scope

This policy applies to all forms of social media, including Facebook, LinkedIn, What's app, Snapchat, X (formally known as Twitter), Wikipedia, all other social networking sites, and all other internet postings, including blogs.

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

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

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, and casual and agency staff (collectively referred to as staff in this policy).

Document Title	Issue No	IMS Ref
SOCIAL MEDIA POLICY	14	P 48



SOCIAL MEDIA POLICY

Third parties with access to our electronic communication systems and equipment must comply with this policy.

3. Personnel Responsible for Implementing the Policy

The Director of Compliance is responsible for the effective operation of this policy. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Director of Compliance with input from the Senior Management Team.

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 reporting and investigating when behaviour falls below acceptable standards.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Social media and other policies are available upon request from the HR Department or through SharePoint or Z drive.

Any misuse of social media should be reported to their line manager. Questions regarding the content or application of this policy should be directed to their line manager for further assistance.

4. 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 breaches our policies in another forum, it will also breach them online. For example, employees are prohibited from using social media to:

- breach our electronic information and communications systems policy.
- breach our obligations concerning the rules of relevant regulatory bodies.
- breach any obligations they may have related 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.
- unlawfully discriminate against other staff or third parties or breach our Equal Opportunities policy.

Document Title	Issue No	IMS Ref
SOCIAL MEDIA POLICY	14	P 48



SOCIAL MEDIA POLICY

- breach our Data Protection Policy and GDPR legislation (for example, never disclose personal information about a colleague online);
- breach any other laws or ethical standards (for example, never use social media falsely or misleadingly, such as by claiming to be someone other than you or making misleading statements).

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. Personal Use of Social Media

Personal use of social media is only allowed during breaks and not permitted during working time.

6. 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.

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. You consent to such monitoring by acknowledging this policy and using 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, logins, recordings and other uses of the systems, as well as keystroke capturing and other network monitoring technologies.

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

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

Document Title	Issue No	IMS Ref
SOCIAL MEDIA POLICY	14	P 48



SOCIAL MEDIA POLICY

7. 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. Your manager may require you to undergo training before you do so and impose certain requirements and restrictions regarding your activities.

Likewise, if you are contacted for comments about the organisation that will be published anywhere, including in any social media outlet, direct the inquiry to the Compliance Department and do not respond without written approval. The use of social media for business purposes is subject to the remainder of this policy.

8. Recruitment

We may use internet searches to perform due diligence on candidates during recruitment. Where we do this, we will act by our data protection and equal opportunities obligations.

9. Responsible Use of Social Media

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

Protecting our business reputation:

- Staff must not post disparaging or defamatory statements about:
 - I. Our people;
 - II. our organisation;
 - III. our clients;
 - IV. suppliers and vendors; and
 - V. other affiliates and stakeholders,

Document Title	Issue No	IMS Ref
SOCIAL MEDIA POLICY	14	P 48



SOCIAL MEDIA POLICY

- but staff should also avoid social media communications that might be misconstrued in a way that could damage our business reputation, even indirectly.
- 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.
- Staff are personally responsible for what they communicate on social media. Remember that what you publish might be available for the masses to read for long (including the organisation itself, future employers, and social acquaintances). Keep this in mind before you post content.
- If you disclose your affiliation as an employee of our organisation, you must also state that your views do not represent your employer's. 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 reflect the professional image you present to clients and colleagues.
- 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.
- 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.
- 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.

Respecting intellectual property and confidential information:

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

Document Title	Issue No	IMS Ref
SOCIAL MEDIA POLICY	14	P 48



SOCIAL MEDIA POLICY

- Do not use our logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without prior written permission.
- 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 Compliance Department before making the communication.
- 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.

Respecting colleagues, clients, partners and suppliers:

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

10. Non-Conformance

Any employee who breaches any aspect of the social media or related policies as outlined in section 4 will be subject to a full and thorough investigation. All breaches will then be dealt with through our Disciplinary Policy Procedures.

11. Monitoring & Reviewing of this Policy

The Compliance Director shall review this policy regularly to ensure it meets legal requirements and reflects best practices.

Signed:

Date: 15/01/2025

Gavin Money

Document Title	Issue No	IMS Ref
SOCIAL MEDIA POLICY	14	P 48



SOCIAL MEDIA POLICY

A handwritten signature in black ink, appearing to read 'Gavin Honey'.

Managing Director

The NWH Group Ltd

Document Title	Issue No	IMS Ref
SOCIAL MEDIA POLICY	14	P 48