

1. INTRODUCTION

- 1.1 This policy is designed to guide staff in making informed, responsible, and professional decisions regarding the use of social media platforms, including but not limited to blogs, wikis, social networking sites, podcasts, video-sharing platforms (e.g., YouTube, TikTok), forums, message boards, instant messaging apps (e.g., WhatsApp, Slack), collaborative platforms (e.g., Google Docs, Microsoft Teams), and comments on online articles. Examples of such platforms include Twitter, Facebook, LinkedIn, Instagram, and other emerging digital platforms.
- 1.2 This policy outlines the standards we require staff to observe when using social media, the circumstances in which we will monitor your use of social media and the action we will take in respect of breaches of this policy.
- 1.3 This policy supplements our **IT & Communications Policy (IT-PL-001)**.
- 1.4 This policy does not form part of any contract of employment and it may be amended at any time.

2. SCOPE

- 2.1 Responsibility for this Policy ultimately lies with the Chief Executive Officer, Van Elle. Day to day implementation of the Policy is the responsibility of the relevant Divisional and department heads. Responsibilities are subsequently devolved, as appropriate, to line managers, HR and the HSQE functions. All employees have a responsibility to comply with this Policy and its associated arrangements.
- 2.2 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, casual and agency staff and volunteers (collectively referred to as **staff** in this policy).
- 2.3 All staff are expected to comply with this policy at all times to protect the privacy, confidentiality, and interests of our company and our services, employees, partners, customers, and competitors.
- 2.4 Breach of this policy may be dealt with under our **Disciplinary Procedure (HR-PR-009a)** and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

3. RESPONSIBILITY FOR IMPLEMENTATION OF THE POLICY

- 3.1 The Chief Executive Officer has overall responsibility for the effective operation of this policy.
- 3.2 The IT Manager is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to our operations.
- 3.3 All staff are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All staff should ensure that they take the time to read and understand it. Any breach of this policy should be reported to the Head of HR.
- 3.4 Questions regarding the content or application of this policy should be directed to a Director.

4. USING SOCIAL MEDIA SITES IN OUR NAME

- 4.1 Only the Main Board are permitted to post or authorise the posting of material on a social media website in our name and on our behalf. Any breach of this restriction will amount to gross misconduct.

5. RULES FOR USE OF SOCIAL MEDIA

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules:

- 5.1 Always write in the first person, identify who you are and what your role is, and use the following disclaimer "*The views expressed are my own and don't reflect the views of my employer*".
- 5.2 Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- 5.3 Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform their Line Manager.

Document Owner: Head of Marketing
Document Number: MKT-PL-014
Date of Issue: 14.09.2025

Document Type: Policy
Page: 1 of 3
Version: 3.0



- 5.4 Ensure that only positive health, safety and environmental site practices are shown in any social media posts related to the Company.
- 5.5 Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with a member of the Main Board.
- 5.6 Do not upload, post or forward any content belonging to a third party unless you have that third party's consent.
- 5.7 It is acceptable to quote a small excerpt from an article, particularly for the purposes of commenting on it or criticising it. However, if you think an excerpt is too big, it probably is. Quote accurately, include references and when in doubt, link, don't copy.
- 5.8 Before you include a link to a third party website, check that any terms and conditions of that website permit you to link to it. All links must be done so that it is clear to the user that they have moved to the third party's website.
- 5.9 When making use of any social media platform, you must read and comply with its terms of use.
- 5.10 Do not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.
- 5.11 Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of us as a company. If you make a mistake in a contribution, be prompt in admitting and correcting it.
- 5.12 You are personally responsible for content you publish into social media tools – be aware that what you publish will be public for many years.
- 5.13 Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset, return to it later when you can contribute in a calm and rational manner.
- 5.14 If you feel even slightly uneasy about something you are about to publish, then you shouldn't do it. If in doubt, always discuss it with a member of the Main Board first.
- 5.15 Don't discuss colleagues, competitors, customers or suppliers without their prior approval.
- 5.16 Always consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics and religion.
- 5.17 Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details.
- 5.18 Before your first contribution on any social media site, observe the activity on the site for a while before launching in yourself to get a feel for the style of contributions, the nature of the content and any 'unwritten' rules that other contributors might follow.
- 5.19 Activity on social media websites during office hours should complement and/or support your role and should be used in moderation.
- 5.20 If you notice any content posted on social media about us (whether complementary or critical) please report it to a member of the Main Board.

6. MONITORING USE OF SOCIAL MEDIA WEBSITES

- 6.1 Staff should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken under our **Disciplinary Procedure (HR-PR-009a)**.
- 6.2 We reserve the right to restrict or prevent access to certain social media websites if we consider personal use to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.
- 6.3 Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and us. It may also cause embarrassment to us and to our clients.
- 6.4 In particular uploading, posting forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

Document Owner: Head of Marketing
Document Number: MKT-PL-014
Date of Issue: 14.09.2025

Document Type: Policy
Page: 2 of 3
Version: 3.0



- (b) a false and defamatory statement about any person or organisation;
- (c) material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to us, our clients or our staff;
- (d) confidential information about us or any of our staff or clients (which you do not have express authority to disseminate);
- (e) any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or
- (f) material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

- 6.5 Any such action will be addressed under the **Disciplinary Procedure (HR-PR-009a)** and is likely to result in summary dismissal.
- 6.6 Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our **Disciplinary Procedure (HR-PR-009a)**, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary, such information may be handed to the police in connection with a criminal investigation.
- 6.7 If you notice any use of social media by other members of staff in breach of this policy please report it to a member of the Main Board.

7. MONITORING AND REVIEW OF THIS POLICY

- 7.1 The Chief Executive Officer shall be responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice.

Signed



Date 14.09.2025

Mark Cutler - Chief Executive Officer

Review Date 14.09.2026

Document Owner: Head of Marketing
Document Number: MKT-PL-014
Date of Issue: 14.09.2025

Document Type: Policy
Page: 3 of 3
Version: 3.0

Think Safe
Act Safe 