Social Media Policy

1. Social media definition

Social media is an interactive online media that allows users to communicate instantly with each other or to share data in a public forum. It includes social and business networking websites such as Facebook, WhatsApp, YouTube, Instagram, WeChat, Snapchat, TikTok, Pinterest, Reddit, Discord, Tumblr, Threads, X and LinkedIn, Google. Social media also covers video and image sharing websites such as YouTube and Flickr, as well as personal blogs. This is a constantly changing area with new websites being launched on a regular basis and therefore this list is not exhaustive.

This policy applies in relation to any social media that employees may use.

2. Use of social media at work

The Company permits employees to make reasonable and appropriate use of social media websites or to keep a personal blog using the Company's IT systems and equipment or their own computers or devices, such as laptops, mobile phones and other hand-held devices, during their normal working hours, provided this does not significantly interfere with their job duties or have a detrimental effect on their productivity. Employees must not spend an excessive amount of time while at work accessing social media websites.

Employees may also be asked to contribute to the Company's own social media activities during normal working hours, for example by writing Company blogs or newsfeeds or managing a social media account for the Company. Employees must be aware at all times that, while contributing to the Company's social media activities, they are representing the Company.

3. Company's social media activities

Where employees are authorised to contribute to the Company's own social media activities as part of their job duties, for example for marketing, promotional and recruitment purposes, they must adhere to the following rules:

- Use the same safeguards as they would with any other type of communication about the Company that is in the public arena.
- Ensure that any communication has a purpose and a benefit for the Company.
- Obtain permission from their line manager before embarking on a public campaign using social media.

- Request their line manager to check and approve content before it is published online.
- Follow any additional guidelines given by the Company from time to time.

The social media rules set out below also apply as appropriate.

4. Social media rules

The Company recognises that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the Company in these circumstances, employees must be aware that they can still cause damage to the Company if they are recognised online as being one of its employees. Therefore, it is important that the Company has strict social media rules in place to protect its position.

When logging on to and using social media websites and blogs at any time, including personal use on non-Company computers and mobile phones outside the workplace and outside normal working hours, employees must not:

- Other than in relation to the Company's own social media activities or other than where expressly permitted by the Company for business networking websites such as LinkedIn, write about their work for the Company – and, in postings that could be linked to the Company, they must also ensure that any personal views expressed are clearly stated to be theirs alone and do not represent those of the Company.
- Conduct themselves in a way that is potentially detrimental to the Company or brings the Company or its employees, clients, customers, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content.
- Other than in relation to the Company's own social media activities or other than where expressly permitted by the Company for business networking websites such as LinkedIn, use their work e-mail address when registering on such sites or provide any link to the Company's website.
- Allow their interaction on these websites or blogs to damage working relationships with or between employees and clients, customers, contractors or suppliers of the Company, for example by criticising or arguing with such persons.
- Include personal information or data about the Company's employees, clients, customers, contractors or suppliers without their express consent (an employee may still be liable even if employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable) – this could constitute a breach of the Data Protection legislation which is a criminal offence.
- Make any derogatory, offensive, adverse, discriminatory, untrue, negative, critical or defamatory comments about the Company, its employees, clients, customers, contractors or suppliers, or any

comments which might reasonably be considered to insult or damage the Company's or their reputation or character (an employee may still be liable even if the Company, its employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable).

- Make any comments about the Company's employees that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying – employees can be personally liable for their actions under the legislation.
- Disclose any trade secrets or confidential, proprietary or sensitive information belonging to the Company, its employees, clients, customers, contractors or suppliers or any information which could be used by one or more of the Company's competitors, for example information about the Company's work, its products and services, technical developments, deals that it is doing, future business plans and staff morale.
- Breach copyright or any other proprietary interest belonging to the Company, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work – if employees wish to post images, photographs or videos of their work colleagues or clients, customers, contractors or suppliers on their online profile, they should first obtain the other party's express permission to do so.

Employees must remove any offending content immediately if they are asked to do so by the Company.

Work and business contacts made during the course of employment through social media websites and which are added to personal social networking accounts amount to confidential information belonging to the Company and accordingly the Company may ask for them to be surrendered on termination of employment.

Employees should remember that social media websites are a public forum, even if they have set their account privacy settings at a restricted access or "friends only" level, and therefore they should not assume that their entries on any website will remain private or confidential.

Employees must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for example by setting their privacy settings at a high level and restricting the amount of personal information they give out, such as date and place of birth, schools attended, family names and favourite football team. This information may form the basis of security questions and/or passwords on other websites, such as online banking.

Should employees observe inaccurate information about the Company on any web sources of information, they should report this to their line manager in the first instance.

5. Social media references

Where employees (or ex-employees) have set up personal profiles on business networking websites such as LinkedIn, these websites may include the facility for the user to request their contacts or other users to provide them with open recommendations, endorsements or references which are then published on their personal profile web pages for other contacts or connections, or prospective contacts or connections, to read. As these could potentially be construed as open references given on behalf of the Company, employees are prohibited from providing these types of recommendations, endorsements or references online to or for the benefit of other employees or ex-employees without the prior permission of their line manager.

If these types of recommendations, endorsements or references are requested online by clients, customers, contractors, suppliers or other Company-related business connections, employees should refer such requests to their line managers.

6. Social media monitoring

The Company reserves the right to monitor employees' use of social media on the internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- Promote productivity and efficiency.
- Ensure the security of the system and its effective operation.
- Ensure there is no unauthorised use of the Company's time, for example to check that an employee has not been spending an excessive amount of time using social media websites for non-work related activity when they should be working.
- Ensure that inappropriate, restricted or blocked websites are not being accessed by employees.
- Ensure that all employees are being treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to harassment contrary to the Equality Act 2010.
- Ensure there is no breach of commercial confidentiality.

The Company reserves the right to restrict, deny or remove internet access, or access to particular social media websites, to or from any employee.

7. Contravention of this policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under the Company's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

The Company will process the personal data collected in connection with the operation of the social media policy in accordance with its data protection policy and any internal privacy notices in force at the relevant time. Inappropriate access or disclosure of personal data will constitute a data breach and should be reported immediately to the Company's Data Protection Officer [Roz Healey] in accordance with the Company's data protection policy. Reported data breaches will be investigated and may lead to sanctions under the Company's disciplinary procedure.

Signed:	
Print name:	Roz Healey, Director, Beech Web Services Ltd
Date:	27/01/25
Date for next review:	27/01/2026