



Social Media Policy

Introduction

This policy applies equally across all Supreme Group businesses (hereafter, “the Company”).

Scope

This policy covers all individuals working at all levels and grades, including full time and part-time employees, fixed-term employees, consultants, contractors, casual and agency staff.

This policy deals with the use of all forms of social media, including but not limited to, Facebook, LinkedIn ,X (formerly Twitter), Instagram, Signal, Telegram, all other social networking sites, and all other internet postings, including blogs.

Attention is drawn to other Company policies regarding the appropriate / inappropriate use of Company supplied devices.

Breaches 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 Company equipment or facilities are used for the purpose of committing the breach. Any employee (or anyone acting on behalf of the Company) suspected of committing a breach of this policy will be required to co-operate with any Company investigation, which may involve handing over relevant passwords and login details. The Company also reserves the right to suspend internet access where it deems it necessary during an investigation. When considering any potential breach of this policy, the Company will consider the context of any social media posting.

Employees (or anyone acting on behalf of the Company) 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.

Responsible use of social media

The following sections of the policy provide employees (or anyone acting on behalf of the Company) with common-sense guidelines and recommendations for using social media responsibly and safely.

Protecting the Company’s business reputation:

Employees (or anyone acting on behalf of the Company) must not post disparaging or defamatory statements about:

- the Company;
- its clients or any member of a client’s staff;
- its employees;

Document Classification		External	
Document Number	Issue Number	Last Review Date	Next Review Date
SG-0023	SG-HR-0023	Jan-2026	Jan-2027



- its suppliers and vendors; and
- members of the public they may have interacted with during the course of their duties.

Employees (and anyone acting on behalf of the Company) should also avoid social media communications that might be misconstrued in a way that could damage the Company's business reputation, even indirectly.

Unless expressly authorised to speak on behalf of the Company, either using a Company social media account or otherwise employees (or anyone acting on behalf of the Company) should make it clear in social media postings they are speaking on their own behalf.

Employees (or anyone acting on behalf of the Company) are personally responsible for what they communicate in social media and should remember that what they publish might be available to be read by a wider audience (including the Company itself, competitors, potential future employers and social acquaintances) for a long time.

If employees (or anyone acting on behalf of the Company) disclose their affiliation as an employee of the Company, unless expressly authorised to speak on behalf of the Company, either using a College social media account or otherwise they must also state that their views do not represent those of their employer. For example, employees could state, "the views in this posting do not represent the views of my employer".

Employees (or anyone acting on behalf of the Company) should avoid posting comments about sensitive business-related topics, such as the Company's or a client's performance or confidential information. Even if it is made clear that their views on such topics do not represent those of the Company or a client, their comments could still damage the Company's or a client's reputation or breach confidentiality obligations.

If anyone 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 line-manager in the first instance.

If anyone see content in social media that disparages or reflects poorly on the Company or its stakeholders, they should report their concerns to their line-manager in the first instance. All staff have a duty of care for protecting the Company's business reputation.

All employees (or anyone acting on behalf of the Company) should use Company e-mail addresses for the conduct of Company business via social media. Use of private e-mail addresses for Company business is prohibited and may be treated as a disciplinary matter.

Responsibilities

All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all employees (and anyone acting on behalf of the Company) understand the standards of behaviour expected of them and for taking the appropriate action when behaviour falls below its requirements.

Document Classification		External	
Document Number	Issue Number	Last Review Date	Next Review Date
SG-0023	SG-HR-0023	Jan-2026	Jan-2027



All employees (and anyone acting on behalf of the Company) are responsible for the effectiveness of this policy and should ensure they take the time to read and understand it. Any misuse of social media should be reported to a line manager or Human Resources.

Monitoring

The contents of the Company's IT resources and communications systems are the Company's property. Therefore, employees (or anyone acting on behalf of the Company) should have no expectation of privacy in any message, files, data, document(s), 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 the Company's electronic information and communications systems.

The Company reserves the right to monitor, intercept and review, without further notice, employee (or anyone acting on behalf of the Company) activities using Company IT resources and communications systems, including but not limited to social media postings and activities, to the extent permitted or as required by law, to ensure the Company's rules are being complied with and for legitimate business purposes and employees (or anyone acting on behalf of the Company) consent to such monitoring by 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.

Review

This policy will be reviewed at least annually or in the event of an incident or breach of policy. Any amendments will be communicated throughout the Company.

Document Classification		External	
Document Number	Issue Number	Last Review Date	Next Review Date
SG-0023	SG-HR-0023	Jan-2026	Jan-2027