LODGE SECURITY

SOCIAL MEDIA POLICY

CONTENTS **Page**

1. PURPOSE

As a security provider, Lodge Security must uphold its reputation and mitigate any risks associated to is employees, customers and the business as far as is reasonably possible.
This policy outlines the standards and expectations for you when using social media, both professionally and personally, to protect your safety, the safety of others and to protect the reputation, confidentiality, and integrity of the company.

2. SCOPE

This policy applies to all employees (full-time, part-time, and temporary), Contractors and subcontractors, Temporary staff and agency workers and any person representing or associated with Lodge Security who use social media platforms in a professional or personal capacity that may put them, others, customers or Lodge Security at risk.

Failure to act in accordance with the Social Media Policy may result in action in accordance with the Company's Disciplinary Policy and Procedure.

Former employees remain bound by confidentiality obligations regarding sensitive information acquired during employment.

3. DEFINITIONS OF SOCIAL MEDIA

Social media includes, but is not limited to:

- Social networking sites (e.g., Facebook, LinkedIn, Twitter/X, Instagram)
- Blogs and microblogs
- Forums and discussion boards
- Video and image sharing platforms (e.g., YouTube, TikTok)
- Messaging apps with public or group features (e.g., WhatsApp, Slack, Discord)

4. USE OF SOCIAL MEDIA AT WORK

You are encouraged to make reasonable and appropriate use of the company's official social media accounts for promoting services, supporting company initiatives and engaging with the public and security sector.

The following types of content are generally appropriate to share when approved through proper channels:

- Company announcements already in the public domain
- Industry awards and certifications
- Company participation in charitable events or community initiatives
- Approved marketing materials and service information
- Industry news and insights (from reputable sources)
- Career opportunities and recruitment notices
- Professional development achievements (e.g., training certifications)
- Company-approved events and photos

The following types of content should not be shared on social media.

- **Confidential or proprietary information** about Lodge Security, its clients, or partners (e.g., contracts, internal communications, operational procedures).
- **Client-specific details**, including names, locations, schedules, or any identifying information.
- **Photos or videos** taken at client sites or of security operations, unless explicitly approved.
- **Security-related information**, such as patrol routes, alarm response protocols, or vulnerabilities.
- **Unverified or speculative information** about incidents, emergencies, or company matters.
- **Negative or defamatory comments** about the company, colleagues, clients, or competitors.
- **Content that violates privacy**, including images or information about employees or clients without consent.
- **Offensive, discriminatory, or inappropriate content**, even if posted in a personal capacity.
- **Political or religious commentary** that could be associated with the company or its values.
- **Any content that could damage the reputation** of Lodge Security or undermine public trust.

Personal use of social media is permitted only during official breaks and must not interfere with your work duties. Don't use your phone or personal device to check social media while on duty unless your manager has authorised.

5. PROFESSIONAL CONDUCT ON SOCIAL MEDIA.

When contributing to the company's social media or referencing the company in any way:

- Always represent the company positively and professionally.
- Do not disclose confidential, sensitive, or proprietary information.
- Avoid sharing specific details such as client names, locations, or schedules.
- Do not post content that could be considered discriminatory, harassing, defamatory, or offensive.
- Obtain managerial approval before launching any public-facing campaign or initiative.
- Do not post photos that reveal security measures or client premises

6. PERSONAL USE AND REPRESENTATION

You may identify yourself as working for the company but when expressing personal views you must include a disclaimer such as: _"The views expressed are my own and do not necessarily reflect those of my employer."_

Your personal social media activity must not bring the company into disrepute.

Don’t get into arguments or post anything negative about the company, your team, clients, or other companies

7. SECURITY AND PRIVACY

Be aware that social media is a public forum. Assume that all content may be seen by clients, competitors, and the public.

- Protect personal and company information to prevent identity theft or data breaches.
- Do not share login credentials or internal systems information

8. INCIDENT RESPONSE AND CRISIS COMMUNICATIONS

Do not comment on ongoing security incidents, emergencies, or negative events involving the company or clients.
If you become aware of negative posts or potential PR issues involving Lodge Security:

- Do not respond personally
- Capture screenshots of the content
- Report immediately to your manager and the communications team

During crisis situations, only authorised spokespersons may communicate on behalf of the company.
Please forward any queries to your manager.

9. RECRUITMENT AND SOCIAL MEDIA

Social media may be used in recruitment only when relevant to the role (e.g., assessing public portfolios or professional presence).

Routine or systematic screening of candidates’ personal social media is discouraged to avoid bias or discrimination.

10. MONITORING AND ENFORCEMENT

To help keep everyone safe and protect the company’s reputation, Lodge Security may monitor how social media is used on company devices or networks.

Please be aware that if someone breaks this policy, it could lead to disciplinary action, up to and including summary dismissal for gross misconduct.

If you see something that doesn’t seem right or might go against this policy, please speak up. You can report it confidentially to your Area Manager or HR.

If you are unsure about any aspect of this policy, consult your line manager or HR.

11. POLICY REVIEW

This policy will be reviewed annually or as required to reflect changes in legislation, technology, or company operations.