

Social Media Policy

All references to Juniper within this document refer equally to Juniper Ventures Limited and Juniper Pursuits Limited

Executive Summary and Introduction

Juniper recognises and embraces the benefits and opportunities that social media can bring. There is, however, an inherent risk involved in using social media, in that, it is an instantaneous and far-reaching form of communication and inappropriate use can impact upon employees and the reputation of the business.

The purpose of this policy is to minimise the risks of social media which can impact on the wellbeing of staff and the reputation of Juniper, so that employees can enjoy the benefits of social networking whilst understanding the standards of conduct expected by Juniper.

Definitions

For this policy, the term “social media” is defined as any type of interactive online media platform that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social forums, anonymous blogs, video and image sharing websites and similar facilities.

Examples include (but are not limited to); Facebook, Instagram, Twitter, LinkedIn, Snapchat, Myspace, Tumblr, WhatsApp and YouTube.

To whom does this apply?

This policy relates to all employees who create or contribute to blogs, social networks, apps, forums, virtual worlds, or any other social media. It should be applied to all use and all forms of social media where there is potential impact on Juniper, whether for work-related or personal use, whether during working hours or otherwise, whether social media is accessed via the company’s IT facilities and equipment, or equipment belonging to members of staff or any third party.

Principles

This policy, like all Juniper policies, is designed to be transparent, accessible and grounded in Juniper’s values:

- **We care:** We treat every colleague with respect, empathy, and fairness.
- **We listen and learn:** We seek to understand concerns and use them to improve.
- **We create together:** We collaborate across teams to support business growth.
- **We are courageous:** We address mistakes openly and take responsible action.
- **We are proud of all we do:** We take ownership for quality and improvement.

Employees should only comment within their own area of expertise to provide individual perspectives on non-confidential activities in the business.

Employees should never represent themselves or the business in a false or misleading way. All statements must be true and not misleading; all claims must be factual and substantiated. Use common sense and courtesy.

Employees should ask permission to publish or report conversations that are meant to be private or internal to the business. Juniper’s privacy and confidentiality guidelines for external communication should not be violated by an employee’s effort to be transparent.

Where employees access social media for work-related purposes or personal use using the company's IT facilities and equipment, Juniper's IT regulations will apply.

Where appropriate, Juniper reserves the right to monitor the use of social media platforms and take appropriate action to protect against any misuse that may be harmful to the company, in accordance with the IT regulations and where the law permits.

Employees should seek guidance before participating in social media when the topic being discussed may be considered sensitive (e.g., a crisis, intellectual property, issues which may impact the company's reputation, commercially sensitive material). Social media activity around sensitive topics should be referred to an Executive Director.

If an employee's use of social media is derogatory, discriminatory, bullying, threatening, defamatory, offensive, intimidating, harassing, creating legal liability for the company, bringing the company into disrepute then the company may act under the staff disciplinary procedure. This may include comments, videos, or photographs, which have been posted on social media sites about the company, employees, work colleagues or managers.

Employees should be aware of security threats and be mindful for phishing attempts. Phishing is a type of social attack often used to steal data, including login credentials and credit card numbers. Social networks can also be used to distribute spam and malware.

Responsibilities

Employees should be transparent and state that they work for Juniper if they are posting about the company. If you are writing about the company or a competitor, use your real name, identify that you work for the company and be clear about your role. Juniper discourages employees from posting online anonymously or using pseudonyms. You should never impersonate another individual.

Policy or Procedure Title	Social Media
Date Adopted by Board of Directors	27 th January 2021
Date last reviewed by Chief Executive Officer	8 th January 2026
Document Identifier	SM – v5 - 20260108
Reviewed by	Michael Hales
Owned by	Philippa Terry
Summary of changes from previous version	v2 - no content changes, reformatted style and document identifier added v3 - no changes other than ownership v4 - periodic review – no changes v5 - added reference to Juniper's Value Framework
Signed Off by Chief Executive Officer/Date	 08-01-2026