Policy details	
Effective Date	16 October 2023
Policy Owners	Group P&C

Version History			
Version	Reason for Release	Date Released	Author
JBS:ERSM:PO:1.0	Endorsed version released	16 October 2023	Group P&C

1. PURPOSE

1.1 This policy outlines the Group's expectations of all Team Members when using Social Media (whether for work or personal use).

1.2 This policy aims to identify and minimise the risks associated with Social Media use (both privately and in connection with work) that might:

(a) impact the reputation or interests of the Group;

(b) cause damage to your employment or commercial relationship with the Group; or

(c) be incompatible with a Team Member's duties and obligations to the Group under any of its relevant workplace policies or any applicable laws (including the Group's Code of Conduct and Ethics, Discrimination, Harassment and Bullying Policy, Privacy Policy and the Competition and Consumer Act 2010 (Cth)).

1.3 This policy is for the mutual protection of the Group, its Team Members and Other Persons and is not intended to unduly prevent, discourage or limit expression of opinion or online activities.

2. SCOPE

2.1 The JBS Australia Social Media Policy applies to Baybrick Pty Ltd and its controlled subsidiaries excluding listed entities (the **Group**) and their employees (**Team Members**) and any Other Persons.

3. DEFINITIONS

3.1 **Authorised Person** – means a person who has been authorised to speak on behalf of JBS.

3.2 **Other Persons** – means anyone who engages in activities at or provides services to the Group in any capacity including:

(a) As a contractor or subcontractor or an employee of a contractor or subcontractor;

(b) An employee of a labour hire company who has been assigned to work at a Group site;

(c) A student gaining work experience; and

(d) A volunteer.

3.3 **Social Media** – the term Social media refers broadly to any online media which allows for user participation, interaction or publishing. Commonly used Social Media tools include without limitation: Facebook, YouTube, Twitter, TikTok, Instagram, Snapchat, Reddit, forums, discussion boards and wikis.

4. POLICY STATEMENT

4.1 The Group:

(a) recognises the value and importance of having an active Social Media presence for communication and engagement with our stakeholders and the wider communities in which we operate;

(b) recognises that Team Members and Other Persons have the right to use Social Media outside of work hours but requires that Team Members and Other Persons understand that online communications have the potential to cause damage to the Group's reputation and interests; and

(c) will educate our Team Members in the appropriate use of Social Media.

5. ACCOUNTABILITIES

5.1 This Policy will be published and reviewed by the Group People & Culture Team in consultation with the Corporate and Regulatory Affairs and the IT Security & Governance teams.

6. POLICY DETAILS

6.1 Social Media should never be used in a way that breaches any of the Group's workplace policies or offends any of the Group's values. If conduct or behaviour on Social Media would breach any of your duties or obligations in another forum, it will also breach those duties or obligations in an online forum.

6.2 When using Social Media on either a Group Social Media account or your personal account, you must not post material that is, or which may reasonably be perceived to be, inappropriate or harmful to the Group, its reputation, its Team Members, Other Persons or any of the Group's stakeholders.

6.3 Without intending to limit your relevant duties and obligations when using Social Media, specific examples include a prohibition on:

(a) posting commentary, content, or images that are unlawful, fraudulent, threatening, bullying, embarrassing, defamatory, pornographic, proprietary, harassing, discriminatory, personally insulting, profanity (whether obscured by symbols or not (i.e. the word example displayed as e#a$ple), ethnic slurs or content that may create a hostile work environment or negatively affect the Group's reputation or relationship with its stakeholders;

(b) publishing, releasing or communicating to others any information that is considered confidential or not publicly available information of the Group including:

(i) information about the Group's operations, business activities, financial position, security, prices or clients;

(ii) Team Member's personal information (including employee ID, addresses and phone numbers); and

(iii) information used to support access to Group IT systems including but not limited to login details or passwords.

6.4 You must ensure that information you publish or communicate about the Group is factually correct and accurate. If information is inaccurate, you must correct that information immediately.

6.5 You must obtain consent from the current or former Team Members, Other Persons or any other external stakeholders of the Group prior to making any reference to, or posting images of the individual/s. Additionally, permission must be obtained to use a third party's copyright, copyrighted material, trademarks, service marks or other intellectual property from the owner of that material.

6.6 You must ensure any content shared on behalf of the Group includes proper credit sourcing when using external sources.

Use of Group Social Media accounts

6.7 Only Authorised Persons can post content on behalf of the Group, or respond to content on behalf of the Group, on Social Media. Group-related Social Media accounts are not to be created without prior written authorisation from the Director – Corporate Communications.

Personal Social Media use

6.8 When using Social Media you may have obligations to the Group that arise:

(a) outside of working hours;

(b) when you are acting in an official and unofficial capacity; and

(c) even when posting material anonymously, or using an "alias" or pseudonym.

6.9 When using Social Media in a private capacity:

(a) You must not use a work email address to register private Social Media accounts;

(b) You must behave in a way that upholds the integrity and good reputation of the Group;

(c) When making comments that relate to the Group or to the type of activities the Group undertakes, you must make it clear that you are expressing your own personal views so that your comments are not perceived to be made on behalf of the Group. You must not use your Group email address or Group logo or insignia as this may give a misleading impression of the Group's endorsement or support of your personal comments;

(d) Where you are identified, or could reasonably be identified, as an employee of the Group, you must be polite and respectful of the opinions of others at all times; and

(e) you must not use Social Media to raise concerns about your employment or other engagement with the Group, or any work-related matter that has potential to damage the Group's reputation and or interests. The appropriate process for raising grievances is detailed in the Group's Complaints and Grievances Policy.

7. MONITORING

7.1 The Group may monitor and review, without further notice, and on a continuous and on-going basis, Team Members activities using its IT resources and communication systems in accordance with applicable policies or procedures. This includes, without limitation, Social Media postings, profiles and activities.

7.2 The Group's IT resources and communications systems include, but are not limited to: computers, storage devices, laptops, tablets, smart phones, internet-based applications and Group social networking applications.

7.3 To avoid any doubt:

(a) monitoring and review can occur anywhere that the Group's IT resources and communications systems are being used, and are not limited to an employee's usual place of work;

(b) monitoring and review includes whether the use of the Group's IT resources and communications systems are for work related or personal use; and

(c) when using the Group's IT resources and communication systems for personal use, Team Members should not assume privacy.

7.4 Team Members should expect that any information they create, post, exchange or discuss on a publicly accessible on-line location may be viewed by the Group at any time. The Group may from time to time conduct audits of Social Media sites to identify breaches of this or any other workplace policy of the Group.

7.5 Team Members are encouraged to report to the Group, any concerns about a potential breach of this or any other workplace policy of the Group. This can be done in accordance with the Group's Complaints and Grievances Policy.

8. PROCEDURES

8.1 Procedures may be made and amended from time to time pursuant to this Policy.

8.2 These Procedures are not intended to be prescriptive, and The Group may elect to deviate from these Procedures if it considers it is reasonable or necessary to do so in the circumstances.

8.3 The Procedures made under this Policy will be read in conjunction with any similar procedure in any applicable industrial instrument. To the extent that there are any inconsistencies between the Procedure and an applicable industrial instrument, the process described in the applicable industrial instrument will be followed.

9. NON-CONTRACTUAL STATUS OF POLICY

9.1 This Policy and any Procedures made pursuant to it is not in any way incorporated as part of any applicable industrial instrument, nor do those documents form any part of a Team Member's contract of employment. The Group may amend this Policy at any time in its sole discretion.

10. QUERIES ABOUT THIS POLICY

10.1 Team Members should contact their designated HR representative in the event of uncertainty about the application of this Policy.

11. BREACHES OF THIS POLICY

11.1 You must immediately report any suspected breaches of this policy to your HR representative or your Leader.

11.2 Breaches of this Policy may result in:

(a) for Team Members, disciplinary action being taken, up to and including termination of employment; and

(b) for all Other Persons, the Group ceasing to engage the person to perform services or undertake activities for or with the Group.

11.3 If a Team Member is suspected of committing a breach of this Policy, they will be required to cooperate with any investigation, which may include preserving and not deleting relevant Social Media content, and providing the Group with reasonable access to content for the purposes of any investigation. A failure to comply with such a direction may in itself result in disciplinary action, including termination of employment.

11.4 Team Members may be required to remove Social Media content, including on a personal Social Media account that the Group reasonably considers constitutes a breach of this Policy. Failure to comply with such a direction may in itself result in disciplinary action, including termination of employment.