SOCIAL MEDIA POLICY

Overview

CIMIC Group Limited and its Operating Companies (**the Group**) recognise the importance of using social media to engage with employees, clients, stakeholders and the community, and that responsible use helps protect the Group's reputation.

Use of social media, including personal use, must comply with all relevant Group policies and procedures, including the *Group Code of Conduct*.

This Policy applies to all direct employees, contractors and third parties engaged by the Group. Failure to comply will amount to a breach of this Policy and may lead to disciplinary action.

What is social media?

Social media is defined as any website or application that enables users to create and share content or to participate in social networking. Common platforms include Facebook, LinkedIn, Twitter, YouTube, Snapchat and Instagram.

This includes internal social media, external social media and personal social media.

Internal social media refers to social media that:

- Is restricted to employees and invited third parties, such as contractors, clients and community members;
- Is approved for use by the Group or is officially managed by the Group; and
- Is not for public view, unless access is granted by an authorised Group representative.

Examples include an intranet-based collaboration site, such as SharePoint, or a closed group on Facebook.

External social media refers to social media that:

- Is open to the public; and
- Is approved for use by the Group or officially managed by the Group.

Examples include Group and Operating Company Twitter and Facebook pages.

Personal social media refers to social media that:

- Is open to the public (either all users of the internet or a selected group of 'friends'/users); and
- Is not Group approved or Group managed.

Examples include personal Facebook, LinkedIn or Twitter accounts.

Conduct and compliance

Users of social media (internal, external, personal)

Users of social media must:

- Familiarise themselves with and understand this *Policy*;
- Ensure they understand and abide by their obligations under the terms and conditions included in all relevant social media, e.g. a specific platform's 'terms of service';
- Recognise the rules that apply to professional and personal conduct in the workplace apply to behaviour on social media;

- Comply with the *Group Code of Conduct* and company policies and procedures, which include but are not restricted to:
  - Behaviour: Workplace behaviour and anti-bullying, harassment and discrimination;
  - Information: Privacy, client and company confidential information, intellectual property and copyright; and
  - Acceptable use of ICT.

Users of social media must not:

- Post or exchange information that may defame, abuse, harass, stalk, threaten or otherwise violate the legal rights of others;
- Publish, post or distribute any defamatory, infringing, indecent, misleading or unlawful material or information;
- Promote, endorse or sell any product or service that is in conflict with the Group;
- Disclose any confidential or sensitive materials outside the Group without permission;
- Use social media to discuss or store any confidential or sensitive client, project or Group information; and
- Use social media to represent the opinion or view of the Group, unless authorised by the CEO.

Personal social media use

Employees should be aware that:

- During work time, personal social media use on the Group's ICT equipment can be monitored in accordance with the *Group Acceptable Use of ICT Policy*. Some reasonable personal use is permitted;
- Outside of work time, personal social media use on personal computers and devices can come to the attention of the Group;
- A communication that is intended as a personal statement and/or limited to a certain audience may find its way into a business or professional context;
- If an individual is identified as an employee, his or her communication may be considered a position or opinion of the Group, even if the intent is personal rather than business and may lead to disciplinary action;
- The Group will discipline employees for any conduct that breaches Group polices/procedures, even if it occurs outside of work time on personal computers and devices; and
- The Group recommends the security settings of personal social media pages are set to 'private'.

Policy Information

Owner:	General Manager Communications, CIMIC
Approved by:	Chief Executive Officer, CIMIC
Version Number:	1.0
Effective date:	14 April 2016 (reformatted 1 November 2016)

Note: CIMIC Group policies may be amended from time to time.