Social Media Procedure

University of Southern Queensland

1 Purpose

To operationalise and support the effective use and management of social media by University Members. This Procedure establishes guidelines and standards for the use, management, and monitoring of social media by University Members, ensuring alignment with University values and regulatory requirements.

2 Scope

This Procedure applies to the use of social media by University Members. The Procedure also outlines how University Members respond to interactions with University social media content by members of the public.

This Procedure should be read in conjunction with the Code of Conduct Policy and the Student General Conduct Policy, which outline overarching expectations for maintaining appropriate standards of conduct and adhering to professional and ethical standards.

3 Procedure Overview

The University's social media presence is managed by Media and Strategic Communications, with official accounts serving as channels for promotion and engagement.

This Procedure outlines processes for University Members engaging on behalf of the University or in a manner that identifies them with the University. The University encourages the responsible use of social media for academic, community, and business engagement, with an emphasis on maintaining a safe, inclusive, and professional environment.

University Members must cooperate with requests to remove any comment, post or other online content where the University forms the view that the content is in breach of this Procedure or the University's expectations. They will be notified by Media and Strategic Communications in these instances.

University social media accounts must clearly indicate that they are maintained by the University and will have University contact information prominently displayed.

Any member of the University community who identifies a suspected fake social media account purporting to represent the University should immediately report this suspicion to Media and Strategic Communications.

Social media account owners are responsible for maintaining an account that adheres to the University's Brand Guidelines and maintains a sufficient level of quality content and engagement as deemed by Media and Strategic Communications.

Media and Strategic Communications reserves the right to restrict where possible, or request the removal of any University social media account or content that is deemed in violation of this Procedure.

Media and Strategic Communications must ensure records related to the use of the University logo, approval of accounts, talent releases, reports and investigations into non-compliance, and any matter related to this Procedure are captured as complete, reliable and accurate evidence of business decisions, actions, recommendations, advice or instruction in relation to social media.

4 Procedures

Official University social media accounts are managed by, or in consultation with, Media and Strategic Communications. Any new social media account representing the University, in whole or in part, must receive prior approval from Media and Strategic Communications. Requests to create a new account must include appropriate justification, confirmation of resourcing to maintain the account, and completion of required social media training. Media and Strategic Communications reserves the right to decline requests for new University social media accounts.

Media and Strategic Communications is responsible for approving any social media account or site that represents the University for promotional purposes, including, but not limited to, accounts promoting University initiatives, research, or events.

At its discretion, Media and Strategic Communications may request the deactivation of any non-official social media channel that seeks to represent the University in any capacity.

4.1 Use of TikTok

The use of the TikTok application at the University is subject to specific guidelines due to significant security and privacy risks associated with the platform's extensive data collection.

The TikTok application must not be installed on University devices. However, access to TikTok via a web interface (e.g., through a browser) on University devices is permitted, provided it complies with other University Policy Instruments. This restriction does not apply to personal devices, however, University data must not be stored on personal devices where the TikTok application is installed, including access to University email accounts.

Legitimate business use of the TikTok application is permitted under limited circumstances, such as for marketing or public relations purposes that align with the University's strategic goals. Media and Strategic Communications must approve all requests to create a University TikTok channel. Requests must include appropriate justification, confirmation of resourcing, and evidence of completed social media

training. Media and Strategic Communications reserves the right to decline such requests.

4.2 Acceptable use of social media

The University encourages and supports its employees to engage on matters directly related to their area of expertise via social media channels. Employees and representatives of the University should be transparent about their identity and role within the institution when engaging on social media.

Employees may only disclose 'public' information. Unauthorised disclosure of non-public information may result in disciplinary actions in accordance with the University's Code of Conduct Policy.

Requests for employees to act as spokespersons on behalf of the University through social media are managed through referral to Media and Strategic Communications. Examples may include tagging UniSQ employees as experts on social media platforms.

For platforms with specific security considerations, such as TikTok, approved business use is permitted only under limited circumstances (e.g., marketing or public relations purposes aligned with University goals). Approved TikTok users must:

- Install the TikTok application only on a standalone device without access to official University information.
- Ensure the standalone device is securely stored and isolated from sensitive data or conversations.
- Remove metadata from photos, videos, and documents before uploading to TikTok.
- Minimize sharing of personal identifying information where possible.
- Use a generic email address for TikTok accounts and ensure multi-factor authentication (MFA) and unique passphrases are in place.
- Regularly review TikTok's terms and conditions and permissions with each update to ensure compliance.
- Delete the TikTok application from devices when no longer needed.

Media and Strategic Communications must approve all requests for University TikTok accounts, including justification, resourcing, and completion of social media training. Media and Strategic Communications reserves the right to decline such requests or revoke approval where necessary.

4.3 Unacceptable use of social media

University Members must align their behaviour with this Procedure when using official University social media channels, engaging with social media in learning, teaching, or research contexts, or making identifiable private use of social media. This includes

adhering to platform-specific requirements, such as those for TikTok, which prohibit the installation of the TikTok application on University devices and require compliance with risk mitigation strategies for legitimate business use.

Non-compliance with this Procedure, including platform-specific requirements such as those for TikTok, may result in a breach of the Code of Conduct Policy or Student General Misconduct Policy. TikTok-specific non-compliance includes the installation of the application on University devices, failure to follow mitigation strategies, or storing University data on devices with TikTok installed.

University Members must not:

- post material or make any comment that is, or might be construed to be, racial or sexual harassment, offensive, obscene (including pornography), defamatory, discriminatory towards any person, or inciting hate;
- post material or make any comment that creates, or might be construed to create, a risk to the health or safety of a student, contractor, employee or other person, including material that amounts to bullying, psychological or emotional violence, coercion, harassment, sexual harassment, aggressive or abusive comments or behaviour, and/or unreasonable demands or undue pressure;
- post material or make any comment that infringes copyright, is fraudulent, breaches intellectual property rights, constitutes a contempt of court or stalking, breaches a court order, or is otherwise unlawful;
- use the University's logo or any other University trademark without prior written permission of Media and Strategic Communications;
- use the University's name, directly or by association, in a manner that is likely to be misleading or bring the University into disrepute;
- imply they are authorised to speak as a representative of the University, or give the impression that the views expressed are those of the University (unless officially authorised by the University);
- use the identity or likeness of another student, contractor, employee or other member of the University community;
- use or disclose any University confidential information obtained as a member of the University community;
- sell, purchase, share, post or offer to write assignments or other assessable work that would be considered a breach of the Student General Conduct Policy; or
- post answers to practice questions, tutorial questions, practice exams or other such material issued by the University.

When using social media, University Members should be aware that:

- Relying on anonymity or pseudonyms does not guarantee protection and could lead to potential breaches;

- liking, sharing or commenting on a post may be seen to be endorsing the content or author, or perpetuating inappropriate social media posts;
- A site's security setting should never be relied upon to protect or keep material private;
- Any online content can be traced back to an individual, potentially revealing their employment or enrolment details; and
- Online comments are available immediately to a wide audience, can last indefinitely, and may be copied and shared out of context.

4.4 Image and video consent

When publishing images or videos on social media, University Members must obtain consent from any identifiable individuals before posting, sharing, or distributing the content. For images or videos involving children, vulnerable adults, research subjects, or clinical patients, additional approvals may be required, such as research ethics clearance or guardian consent.

4.5 Monitoring

Social media account owners are responsible for maintaining the account/s, including monitoring all posts.

Social media account owners are responsible for deleting comments or content deemed defamatory, inaccurate, false, misleading, in breach of University Policy Instruments, or that may negatively affect the reputation of the University. Comments or content of this nature should be recorded (via a screenshot before being deleted) and may need to be escalated to the relevant University portfolio should it be in breach of a policy. University Members are required to cooperate with requests from Media and Strategic Communications to remove any content that breaches this Procedure or the University's expectations.

4.6 Social media training

All University Members managing University social media accounts must complete social media training provided by Media and Strategic Communications before commencing activities. TikTok-specific training will include guidance on mitigation strategies, security practices, and content management. Media and Strategic Communications has the final authority to permit social media activities, including TikTok use, upon completion of training.

4.7 Teaching and learning

Social media channels may be used as supplementary communication tools in a learning and teaching context, alongside other official modes of student communication, including, but not limited to, University email and posts in the University's learning management system. Learning and teaching-related social media channels must be accessible only to relevant students.

4.8 Research

Social media can be effective in improving research impact but should form part of a broader strategy.

University Members who wish to use social media in the conduct of research, and who want an association with the University brand, must consult with Media and Strategic Communications and the Office of Research, to determine the appropriate strategy.

4.9 Access controls

Passwords for official University social media channels must be centrally managed by Media and Strategic Communications and immediately reset if an administrator leaves the University.

4.10 Records management

All social media activity related to official University accounts, including posts, comments, images, and videos, must comply with the University's Records and Information Management Policy. University Members responsible for social media accounts are required to retain records of significant interactions, approvals, and any instances of removed or restricted content.

For content requiring additional approvals, such as images or videos of identifiable individuals, records of consent and any additional clearances (e.g., research ethics approval or guardian consent) must also be maintained in line with the University's record-keeping standards.

5 References

Nil.

6 Schedules

This procedure must be read in conjunction with its subordinate schedules as provided in the table below.

7 Procedure Information

Accountable Officer	Pro Vice-Chancellor (Engagement)
Responsible Officer	Director, Media and Strategic Communications
Policy Type	University Procedure
Policy Suite	Social Media Policy

Subordinate Schedules	
Approved Date	
Effective Date	
Review Date	
Relevant Legislation	
Policy Exceptions	Policy Exceptions Register
Related Policies	Academic Freedom and Freedom of Speech Policy Acceptable use of ICT Resources Policy Code of Conduct Policy Media Engagement Policy Student General Conduct Policy
Related Procedures	Student General Misconduct Procedure
Related forms, publications and websites	
Definitions	**Terms defined in the Definitions Dictionary**
	Definitions that relate to this procedure only
	Social Media A broad term that encompasses interactive online communication channels that enable users to create and share content, opinions, experiences, and knowledge. These can be written comments, videos, photographs, or audio files. Social media channels may include, but are not limited to, Facebook, Instagram, X (Twitter), YouTube, LinkedIn, and TikTok. **Official University Social Media** Refers to any public social media account, group or site that seeks to represent the University as a whole or in part for promotional purposes, including (but not limited to) promoting University initiatives, research or events. Official University social media channels are managed by, or in consultation with, Media and Strategic Communications. **Identifiable Private Use of Social Media** The use of social media in a way that may associate the user

	with the University and/or impact the University or members of the University community. **Non-identifiable Private Use of Social Media** The use of social media by a member of the University community in a way that does not associate the user with the University and does not impact the University or a member of the University community in ways that could be reasonably considered inconsistent with the Code of Conduct Policy or Student General Conduct Policy.
Keywords	
Record No	23/579PL

Drafting version control
(to be removed prior to provision to final approval authority and publication to Policy and Procedure Library)

Version	Date	Author	Change Description