

# Social Media Use Policy for Staff

April 2022 - This document is rescinded and is replaced by the [Communications and Marketing Policy](#) and [Communications and Marketing Procedure - Media, Engagement and Public Comment](#).

## Section 1 - Purpose

- (1) This document sets out Charles Sturt University's (the University) policy on staff members' professional and personal use of social media and the use of University computing and communication facilities to participate in social media forums.
- (2) This Policy aims to encourage participation in social media in a responsible and respectful manner to ensure that:
- the reputation of the University is maintained and enhanced;
  - use complies with Australian and international laws and the rules, regulations and policies of the University, particularly relating to prohibited data or material, harassment and discrimination, threatening behaviour, libel, defamation, privacy, and the protection of intellectual property; and
  - all participation complies with the terms of use of the relevant social media platform.

### Scope

- (3) This Policy applies to:
- all staff members of the University; and
  - persons who hold a visiting or adjunct appointment with the University; and
  - associates of the University.

## Section 2 - Glossary

- (4) For the purpose of this Policy:
- Electronic information - means information stored, issued, distributed or forwarded as text, graphics, images, animations, video, sound and/or computer programs.
  - Personal use of social media - means individual or private use of social media platforms, using their own personal social media accounts, including to socialise online, send messages, share interests and information, chat, meet people, and post information, photographs and videos.
  - Professional use of social media - includes the use of social media platforms to facilitate the teaching, research, marketing, recruitment, administration or authorised commercial activities of the University. For example, lecturers are encouraged to make use of relevant online forums as part of the learning environment.
  - Social media platforms - refers to applications, websites or tools that enable people to socialise online, send messages to one another, share interests and information, chat, meet people, and post information, photographs and videos for others to look at. These platforms may be internal or external, and include:
    - social and professional networking sites, e.g. Facebook, Yammer, LinkedIn and Google+;
    - video and photo sharing sites, e.g. Flickr, YouTube and Vimeo;

- iii. blogs (weblogs) and blogging platforms, e.g. WordPress, Blogger and Tumblr;
- iv. micro-blogging and activity stream sites, e.g. Twitter;
- v. forums and discussion boards, e.g. Trove Forum, Yahoo Groups and Google Groups;
- vi. collaborative online deliberation and argument map sites, e.g. Debategraph;
- vii. virtual communities, e.g. Second Life;
- viii. wikis (collaboratively created repositories of content), e.g. Wikipedia; and
- ix. and other application, website or tool that allows for user generated content exchange.

## Section 3 - Policy

### Related Documents

(5) Internal policy documents that specify acceptable standards of conduct in relation to the use of social media include:

- a. Social Media Use Procedure for Staff;
- b. [Social Media Guidelines](#);
- c. [Code of Conduct](#);
- d. [Harassment and Bullying Prevention Policy](#);
- e. [Privacy Management Plan](#);
- f. [Intellectual Property Policy](#);
- g. [Communications and Marketing Procedure - Media, Engagement and Public Comment](#);
- h. [Communications and Marketing Procedure - Website and Social Media Platforms](#); and
- i. [Computing and Communications Facilities Use Policy](#).

### General Principles

(6) The University is committed to encouraging freedom of expression, public comment and engagement of staff in intellectual debate and cultural pursuits in a consistent and professional manner in all forms of media.

(7) Staff are expected to read, understand and comply with University policies relating to the use of computing and communication facilities, public comment and staff conduct.

(8) Staff must not deliberately publish any misleading or incorrect information or make any misleading or incorrect comments on social media.

(9) Staff must not use social media to make comments that may damage the reputation of the University or any members of the University community (e.g. staff, students, alumni, community or business partners).

(10) Staff are personally responsible and will be held accountable for any content or comments that have a connection with the University, which they publish on social media platforms. This applies to content and comments published on their personal social media platforms and on the platforms of others, either in a professional or personal capacity.

(11) Social media posts are broadcasts. Even if you intend to broadcast a message to only a few people, social media posts are a permanent record in the public domain. They can be searched, shared, stored, and spread globally, even when the content has been deleted. This may result in consequences that the staff member did not intend. It is therefore important for staff to ensure the appropriateness of their content, and to use privacy settings to review and approve comments before they appear. Staff should monitor their comments and posts regularly, and respond appropriately (e.g. deleting offending comments from the platform and/or blocking users).

(12) The University accepts no responsibility for the content of external social media platforms that are "followed", "tagged" or referenced by/on an official University social media platform. "Following", "tagging" or referencing does not constitute endorsement by the University.

(13) Information posted on the University's social media platforms by external users does not constitute endorsement by the University.

## **Professional Use of Social Media**

(14) Staff must not make any comments on behalf of the University, or that might be perceived as being made on behalf of the University, unless they have delegated authority to do so. An authorised representative should disclose their name/position title and the fact that they are communicating the views of the University officially.

(15) If a staff member comments in a professional capacity on a subject that relates directly to their University appointment but they are not commenting on behalf of the University, then they may give the title of their University appointment in order to establish their credentials. They should also include a disclaimer that the views expressed are their own and not those of the University.

(16) Staff must not continue to use, access or assert ownership over any social media platforms that they were authorised to use as a staff member after they have ceased employment with the University (e.g. by closing, transferring or renaming a University Twitter account).

## **Personal Use of Social Media**

(17) This Policy applies to personal use of social media where there is a connection with the University. Circumstances in which there is a connection with the University include where:

- a. the social media platform is established or used as an authorised University social media platform, e.g. CSU Facebook, Twitter or LinkedIn sites; or
- b. the social media platform is accessed using University computing or communication facilities (including remote access facilities) either during normal working hours or after hours; or
- c. a person identifies themselves as a University staff member on the platform or they can be directly or indirectly associated with the University (referred to as "identifiable personal use"); or
- d. the content of the social media platform is specifically about the University or any members of the University community, e.g. University ranking/rating websites, or comments about colleagues, students or supervisors.

(18) Staff must not make comments on social media that might be interpreted as being made on behalf of the University unless they are authorised to do so. If staff make unauthorised comments related to the University, they should include a disclaimer clearly stating that they are not commenting on behalf of the University. For example, "These are my personal views and do not necessarily represent the University's policies, positions or strategies."

(19) In any personal comments that staff make, they should not include their University position title or contact details (e.g. their University telephone number or email address).

(20) Staff must not use the University logo or any other University marks or images (including images of University buildings or facilities) for personal use on social media.

(21) Staff must not use the University's name to promote or endorse any non-University business, product or cause, or any political party or candidate.

(22) All staff members should consider carefully the extent to which they use their personal social media platform for interactions with staff and students. For example, it may not be appropriate for a staff member to use a social media platform to discuss a work issue. A staff member should also consider carefully whether they are willing to accept

students as social media "friends" as this might be perceived as a conflict of interest.

(23) Staff should avoid posting personal revelations and comments or embarrassing photographs on social media platforms. These may be detrimental to their current or future career or have implications on relationships with fellow staff members and students.

## **Use of University Computer and Communication Facilities**

(24) Staff may only use University computing and communication facilities to engage in personal social media activity where such use has:

- a. no negative impact on the performance of their duties (e.g. they may update their Facebook page during their lunch hour but not spend excessive time using social media during their normal working hours); and
- b. no negative impact on the University's information technology facilities.

(25) Use of University computing and communication facilities includes use of remote access facilities provided by the University (e.g. Thin Client) even if the hardware used (e.g. computer or mobile telephone) is not provided by the University. It does not include use of information technology facilities such as audio or video streaming services.

(26) Staff are responsible for any use of their access privileges to the University's computing and communication facilities by anyone other than themselves, e.g. family, friends or household members.

(27) The University may audit and monitor staff usage of University computing and communication network and facilities. This may result in directing a staff member to remove any published content (including comments, images and videos) that has the potential to damage the reputation of the University or University staff or that does not meet the requirements of this Policy.

(28) The University may restrict staff access to specific Internet sites, including social media platforms (e.g. malicious websites).

(29) The University may remove or disable access to devices connected to the University network if they represent a threat to the security of the network (e.g. ransomware, viruses and malware).

(30) Some social media platforms such as YouTube involve high-bandwidth usage. Staff must not access these platforms or download large files for personal use as the University may have to pay an additional amount for usage over a certain limit. Where personal use of social media platforms on University computing and communication facilities has been excessive, the University may request compensation for such access.

## **Legal Responsibilities**

(31) When using social media for professional purposes or for personal use where there is a connection with the University, staff must comply with:

- a. all relevant Australian and international legislation; and
- b. the terms and conditions of use of the relevant social media platform.

(32) Staff must not conduct, encourage or engage in illegal activity (e.g. music or video "piracy").

## **Privacy and Confidentiality**

(33) Staff must ensure the protection of the privacy of individuals and information concerning individuals where that information has not been expressly authorised for release.

(34) Staff must not use social media to publish or report on confidential information about the University or personal

information about students, alumni or fellow staff members obtained in the course of their employment with the University. They should only publish information that is publicly available. The best way to do this is to link to the original source of the information.

### **Copyright and Intellectual Property**

(35) When using social media, staff must not publish information or link to information or platforms that may breach the legal ownership rights of others (e.g. copyright, trademarks or intellectual property).

(36) To avoid plagiarism or breach of copyright, material posted on social media platforms should reference or cite sources of information appropriately.

### **Bullying, Harassment and Discrimination**

(37) Staff must not comment on or publish information that promotes, fosters or perpetuates discrimination on the grounds protected under relevant anti-discrimination or equal opportunity legislation.

(38) Staff must not use social media to make offensive or abusive comments about or to stalk, threaten, harass or intimidate any person. This may amount to cyber-bullying, which could result in disciplinary proceedings or criminal proceedings under the [Criminal Code Act 1995](#).

### **Defamation**

(39) Staff must not make comments or publish information that may damage another person's reputation.

### **Offensive or Obscene Material**

(40) Staff must not post, display, receive, publicise or comment on materials or links to materials that are offensive or obscene (e.g. sexually explicit or pornographic material).

### **Freedom of Information**

(41) The [Freedom of Information Act 1982 \(Cth\)](#) applies to social media content. Content must therefore be able to be managed, stored and retrieved in accordance with this Act.

(42) All University social media platforms will clearly indicate that any content posted or submitted for posting are subject to public disclosure.

### **Breaches of This Policy**

(43) Any alleged breaches of this Policy will be investigated in accordance with the misconduct/serious misconduct provisions in the relevant industrial instrument, and may result in disciplinary action or termination of employment.

(44) The University may direct staff to remove material for which they are responsible (e.g. posted by them) from any social media platform over which they have control (e.g. their Facebook page) if it is in breach of this Policy and/or to take reasonable steps to seek its removal from any social media platform over which they do not have control (e.g. by requesting that the platform moderator remove the material).

(45) The University may decide to take legal action against a staff member for breaches of this Policy.

(46) The University may report any conduct that breaches this Policy to the police or any other appropriate authority external to the University (e.g. the Australian Communications and Media Authority).

## Section 4 - Procedures

(47) Refer to the Social Media Use Procedure for Staff.

## Section 5 - Guidelines

(48) Refer to the [Social Media Guidelines](#) for acceptable standards of conduct in relation to the use of social media.

## Status and Details

<b>Status</b>	Historic
<b>Effective Date</b>	17th February 2016
<b>Review Date</b>	13th October 2018
<b>Approval Authority</b>	Executive Director, Human Resources
<b>Approval Date</b>	2nd February 2016
<b>Expiry Date</b>	5th April 2022
<b>Unit Head</b>	Maria Crisante Executive Director, People and Culture
<b>Author</b>	Malcolm Wilson
<b>Enquiries Contact</b>	Division of People and Culture +61 2 63384884