Social Media Guidelines

DOCUMENT REFERENCE:	**PPP145**
RESPONSIBLE MANAGER:	Manager, Brand and Strategic Marketing
CATEGORY:	Governance
DATE APPROVED:	13/05/2026
DATE OF NEXT REVIEW:	May 2028
RELATED POLICIES/DOCUMENTS:	PPP149 Student Code of Conduct PPP149b Student Code of Conduct - Addendum PPP083 Staff Code of Conduct PPP108 Media Communication Guidelines PPP116 Use of ICT Facilities and Services Guidelines ICT Acceptable Use Policy Information Security Policy Records Management Policy Any future SWTAFE Artificial Intelligence or Digital Ethics policy

1. Introduction

South West TAFE (SWTAFE or the 'Organisation') recognises that social media is an integral communications channel that provides opportunities for interactive two-way communications. It can complement existing communication and further promote information, access and delivery of key services. SWTAFE utilises social media to connect with students, employees, alumni, followers and internally, within the organisation.

This Guideline intends to provide an understanding of and guidance for, the appropriate use of social media platforms and tools. This Guideline outlines how the values and brand of SWTAFE should be demonstrated within social media and guides your participation in this area, whether you are acting on behalf of SWTAFE or participating personally.

SWTAFE recognises the benefit of a social media Guideline ensuring employees – whether using social media is in their role, or in a personal capacity - have guidance as to the organisation's expectations where social media engagement is about SWTAFE, its products and services, its staff and its competitors. SWTAFE encourages employees to act as advocates for the SWTAFE brand on social media.

2. Scope

This Guideline applies to any SWTAFE staff, students, contractors, consultants and Board members who use social media on behalf of SWTAFE, who indicate, through personal information disclosed on their online profile that they are, or may be taken to be a representative of SWTAFE in communicating with or about SWTAFE staff, students or business entity.

This Guideline does **not** apply to an employee or student's personal use of social media platforms where **no** reference is made to SWTAFE related issues.

3. Purpose

This Guideline provides clarity about who you are **representing,** who is **responsible** for ensuring that any references to SWTAFE are factually correct and accurate, and that **respect** is shown to staff, students, the interacting individuals and communities.

Social media and social networking are online services and tools used for publishing, sharing and discussing information. The list of social media platforms is extensive with new and innovative social media platforms being developed constantly.

There are multiple social media platforms that SWTAFE utilise.

Our current official channels are:

Facebook	facebook.com/swtafe	@swtafe
Instagram	instagram.com/swtafe	@swtafe
LinkedIn	linkedin.com/company/swtafe	
YouTube	youtube.com/swtafevic	
TikTok	Tiktok.com/@swtafe.vic	

This list is provided as a guide to some of the different types of social media platforms currently available. However, the absence of a reference to a particular site or type of social media platform **does not** limit the application of these guidelines.

- *Social networking sites*: A social networking site is an online platform that allows users to create a public profile and interact with other users on the website. E.g. Facebook, LinkedIn, Instagram, TikTok, YouTube etc.
- *Video, audio and media sharing websites:* A website that lets people upload and share their video clips, or audio and media files with the public at large or to invited guests. E.g. YouTube, Vimeo, SoundCloud, Viddler, Ustream
- *Blog (short for web log):* A blog is a discussion or informational website published on the World Wide Web consisting of discrete, often informal diary-style text entries or posts. A blog may be anonymous or you can choose to identify yourself. E.g. WordPress, Wix, Medium, Blogger, Tumblr
- *Microblog:* A social media site to which a user makes short, frequent posts often announcing regular updates. E.g. Threads, Viva Engage
- *Location-based services*: Applications which use real-time geo-data from a mobile device or smartphone to provide information, entertainment or security. Some services allow consumers to "check in" at restaurants, coffee shops, stores, concerts, and other places or events. E.g. Facebook, BeReal Instagram, MapMyFitness, Strava and Snapchat
- *Wikis*: A website or database developed collaboratively by a community of users, allowing any user to create, edit and add content. E.g. Wikipedia, Wikispaces
- *Online gaming*: Sites or programs that offer the action or practice of playing video games or role-playing games on the internet. E.g. Fortnite, League of Legends, Counter-Strike, World of Warcraft
- *Forums or message boards:* An internet forum, or message board, is an online discussion site where people can hold conversations in the form of posted messages. They differ from chat rooms in that messages are often longer than one line of text, and are at least temporarily archived. E.g. Reddit, Quora, Stack Overflow

Victorian Government Guidelines on the use of TikTok

The latest Victorian Govt guidelines must be adhered to for the use of TikTok:

https://www.vic.gov.au/administrative-guidelines-improving-cyber-security-victorian-government-systems-and-data#4-guidelines-on-the-use-of-tiktok

Public service bodies and public entities must prevent installation and remove existing instances of TikTok on government devices unless a legitimate business reason exists.

Public service bodies and public entities should update internal information technology and/or security policies and are encouraged to implement technical controls to prevent the use of TikTok on government devices.

Where TikTok needs to be removed by employees, contractors or consultants on Victorian government issued or owned devices, public service bodies and public entities should give reasonable and lawful directions for the person to do so.

Legitimate business use reasons for the TikTok application

Legitimate business use means a need to install or access the TikTok application on a government device to conduct business and/or achieve a work objective of a body or entity. TikTok should only be accessed or installed after an adequate risk assessment has been completed, mitigation strategies are implemented, and necessary internal agency approvals are provided.

Legitimate business use reasons may include:

- where the application is necessary for the carrying out of law enforcement and regulatory functions, including compliance and enforcement functions
- where an entity requires research to be conducted or communications to be sent to assist with a work objective (for example, releasing government communications, countering mis- or dis-information), or
- where an entity must use the application to reach key audiences to undertake education, child safety, staff safety, marketing or public relations activity on behalf of the entity.

Public service bodies and public entities may identify a legitimate business use that requires the installation or ongoing presence of TikTok.

The relevant agency head of the public service body or public entity should ensure legitimate business use reasons are approved by the Chief Security Officer (or equivalent) of the body or entity and ensure the approved risk mitigations are in place:

- ensure TikTok is installed and accessed only on a separate government issued, standalone device without access to services that process or access official and classified information
- ensure the separate, standalone device is appropriately stored and secured when not in use. This includes the isolation of these devices from sensitive conversations and information
- ensure metadata has been removed from photos, videos and documents when uploading any content to TikTok
- minimise, where possible, the sharing of personal identifying content on TikTok
- use an official generic email address (for example, a group mailbox) or Chief Security Officer (or equivalent) approved email account for each TikTok account
- use multi-factor authentication and unique passphrases for each TikTok account
- ensure that devices that access the TikTok application are using the latest available operating system to control individual mobile application permissions
- regularly check for and update the application to ensure the latest version is used
- only install TikTok from trusted stores such as Microsoft Store, Google Play Store and the Apple App Store
- ensure only authorised users have access to corporate TikTok accounts and that access (either direct or delegated) is revoked immediately when there is no longer a requirement for that access
- an appropriately qualified person regularly reviews the terms and conditions of use or installation of TikTok, as well as application permissions with each update, to ensure appropriate risk management controls can be put in place or adjusted as required
- delete TikTok from devices when access is no longer needed.

3.1 Artificial Intelligence (AI)

Artificial Intelligence refers to technologies or tools that generate, analyse, summarise or modify content, including text, images, audio, video or data. This includes generative AI tools, automated publishing tools, platform-embedded AI features, analytics tools and chat or response automation.

4. Clarification and Interpretation

If clarification or interpretation of any aspect of these Guidelines or how it applies to your circumstances is required, please contact the Manager of Brand and Strategic Marketing.

5. Communication and Language

The aim of social media is to promote conversation, maintain communication and enable information sharing. This should be conducted in a safe manner and should not be used as a ground for bullying or promoting personal agendas.
Users who post the following material on a SWTAFE platform will have their posts deleted and may warrant being banned from accessing the social pages and/or being reported to the platform.

- abusive, threatening, defamatory or obscene material
- fraudulent, deceptive or misleading material
- bullying (including, but not limited to making threats, spreading rumours, attacking someone verbally, and excluding someone from a group)
- harassment, including unwanted and annoying actions of one party or a group, including threats and demands (including but not limited to racial, religious, sexual orientation, physical characteristics, gender, ability, disability, or economic status harassment)
- threatening and/or intimidating comments
- promoting hate of any kind
- potentially libellous or defamatory material
- detrimental in any way to another person or organisation
- otherwise offensive or inappropriate impersonating by using another person's online profile to access social networking
- intimidating or threatening material
- not related to the subject matter of the blog, forum, board or site
- including Copyright or Trade Mark protected materials
- in violation of any intellectual property right of another
- in violation of any law or regulation
- advertising materials or offers to sell goods or services, contents, chain letters, spam or any unsolicited commercial message

6. Managing the Community

SWTAFE staff members should take measures to ensure audiences enjoy their user experience on our social media platforms.

- **Responsibility**

  Social media is a medium of conversations, and topics will sometimes arise that require appropriate commentary or responses, as social media conversations are public by nature. If you see any cases of negative feedback or criticism against SWTAFE or bullying or abuse occurring on any of SWTAFE's social media accounts, you have a responsibility to notify the Manager of Brand and Strategic Marketing.

- **Authority to Post**

  SWTAFE has strict limitations on which staff have authority to post, and this is limited to staff within the SWTAFE Marketing Department and Internal Communications Officer on Student groups. These staff are responsible for posting across SWTAFE's various social media accounts for business purposes. Business related posts should only be made by one of these authorised representatives.

  If you wish to suggest content that may be relevant to the SWTAFE social media platforms, you can send this content to the Marketing Department for review to post on the SWTAFE social media accounts.

- **Use of Artificial Intelligence and Automation**
  The use of Artificial Intelligence or automated tools in the management of SWTAFE social media accounts must be controlled and approved.

  - AI tools may be used by authorised Marketing staff to assist with:
    - drafting content
    - scheduling posts
    - analysing engagement or performance data
  - AI tools must **not** be used to:
    - publish content without human review
    - automatically respond to comments, messages or direct enquiries
    - engage in conversations on behalf of SWTAFE without prior approval
  - Fully automated posting, commenting or direct messaging on official SWTAFE social media accounts is **not permitted** unless explicitly approved by the Manager, Brand and Strategic Marketing, in consultation with ICT and Risk & Compliance where required.

- **Timing**

  Audience questions, suggestions and criticism on social media posts and pages should receive professional feedback on the same day. Most consumers expect to receive a quick response to a query posted on social media and as a result, SWTAFE must have a system in place that allows for such responses. Response time can be visible to all visitors therefore an acceptable response should be provided as soon as possible.

- **Removing content**

  If you need to block a user or remove their contribution, do so following a personal communication (provided the user is registered) E.g. "Hello <name>, due to infringements to our guidelines (or legal reasons) we are obligated to delete your comment."

- **Professionalism**

  Don't react emotionally to criticism or questions. Act professionally. Whatever the problems are, we need to address them. Our response should tackle the problem professionally and constructively, rather than becoming defensive or ignoring the comment. If the issue is genuine, acknowledge the problem and demonstrate an intention to find a resolution.

- **Accuracy**

  Never present information that can't be checked or verified. On the internet, information can be verified immediately. False statements or even omissions are exposed straight away. Disclose your sources. This shows respect for the author and increases your credibility.

- **Use of AI-generated content**

  Where Artificial Intelligence tools are used to assist in drafting or generating social media content, the authorised staff member remains fully responsible for ensuring the accuracy, legality, appropriateness and compliance of the content with this Guideline and all related SWTAFE policies prior to publication.

  AI-generated content must not be published without human review and approval.

If there is any doubt about applying the provisions of these guidelines, please check with the Marketing Department before using social media to communicate.

7. Staff

- **Access to SWTAFE social media accounts**
  - Members of the Marketing Department will be responsible for the access and usage of SWTAFE's social media accounts. When a new marketing staff member commences, they will be provided access relevant to their job duties within 7 days. When the staff member departs, they will be removed from accessing social media accounts immediately.
  - All passwords will be stored on the server to ensure accessibility after a staff member's departure. If there is suspicious activity from an account, all passwords will be changed immediately.
- **Staff responsibilities for use of social media**
  - Wherever in doubt, seek advice from the Marketing Department and delay posting information that you are unsure of
  - Under **no** circumstances should staff "follow", request or accept a "friend request" from a student of SWTAFE
  - **Do not** use a work email address to register a personal social media account
  - **Do not** use a personal email address to register a SWTAFE social media account
  - **Do not** make comments outside your area of expertise
  - **Do not** commit SWTAFE to actions or undertakings
  - Only discuss publicly available information. **Do not** disclose confidential information, internal discussions or decisions of the Organisation. This includes publishing confidential, personal or private information where there is sufficient detail for potential identification of SWTAFE staff, students or third parties
  - When using social media do not make comments regarding SWTAFE and its business unless authorised to do so.
  - Ensure you clearly state the views stated on social media platforms are your own.
  - Be accurate, constructive, helpful and informative
  - **Do not** publish any information or make statements which you know to be false or may reasonably be taken as misleading or deceptive
  - Be clear about professional identity or any vested interests
  - Clearly separate personal opinions from professional ones. Be mindful of the Staff Code of Conduct when discussing or commenting on matters of the Organisation
  - Be sensitive to the privacy of others. Seek permissions from anyone who appears in any photographs, video or other footage before sharing these via any form of social media
  - **Do not** comment, contribute, create, forward, post, upload or share content that is malicious or defamatory. This includes statements which may negatively impact on the reputation of another
  - **Do not** publish content in exchange for a reward of any kind
  - **Do not** endorse any political affinity or allegiance
  - Always be courteous, and respectful of others' opinions including detractors
  - **Do not** issue statements or make announcements through social media channels unless authorised. Refer to *PPP108 Media Communication Guidelines.*
  - Staff must not input confidential, personal, student, staff or commercially sensitive information into Artificial Intelligence tools, including generative AI platforms, for the purpose of drafting or generating social media content.
  - Information entered into AI tools may be stored or reused outside SWTAFE's control and must be treated as public unless formally approved otherwise.

- Staff must ensure that any AI-generated text, images or video do not infringe copyright, intellectual property rights, trademarks or platform terms of use.
- The use of AI tools does not diminish individual accountability for content published on, or associated with, SWTAFE social media platforms.

- **Staff opportunities for use and management of social media platforms**
  - Specific Facebook groups can be made for the purpose of communicating with students within class groups:
    - These groups **must** go through the Marketing Department for approval, set up, moderation and evaluation in partnership with the relevant Teaching Division staff
    - Screening questions will be set up to ensure that only current students join the group
    - The groups will be administered by the relevant Teaching Division staff who must follow the guidelines contained in this Guideline
    - Once the group is set up, the link can be shared with students encouraging them to join. Teaching staff are responsible for ensuring that only current students join the group
    - All comments, posts and communications will be accessible by all staff with access to the page
    - All groups will be moderated by teaching staff, ensuring no unacceptable comments, posts, pictures and or videos are posted to the group
    - All groups created will have the highest level of privacy settings ensuring others (outside of the group) cannot see the page content. This ensures the confidentiality of all students and staff
  - If you are using SWTAFE provided services made available to you as an employee or contractor (such as email, smart phone, tablet, internet access and instant messaging) limited personal use of social media is allowed, however it must be within reasonable limits and not interfere with your work;
  - In the event that a problem (including any unacceptable and inappropriate content as outlined above) arises on a SWTAFE social media account, the following people should be advised:
    - Marketing Department – Manager Brand & Strategic Marketing
    - Head of Division (teaching)/Department Manager
    - Student Wellbeing Officer (if appropriate)

    Appropriate steps will then be taken to resolve the issue. Staff should not attempt to resolve the issue over social media.

- **Staff will act in SWTAFE's best interest and value SWTAFE's reputation**

  Employees must:

  - refrain from making any derogatory, disparaging or defamatory comments either verbally, in writing or any form of electronic media, including social media, about SWTAFE, its business and any separate entities associated with SWTAFE's business or operation.
  - respect that confidentiality and information management extends to all written and published documentation and all forms of electronic media, including social media
  - not take any action, or fail to take any action, that may be a breach of the law, the Code of Conduct or any other SWTAFE policies, procedures or practices

8. Students

- **Student Responsibilities for use of Social Media**
  - Students should not attempt to “follow”, request or accept a “friend request” from a staff member of SWTAFE
  - Swearing, harassment, bullying, physical and/or verbal assault including face-to-face or via cyber-communication will not be tolerated as stated in the *PPP149 Student Code of Conduct & PPP149b Student Code of Conduct addendum.*
  - Be sensitive to the privacy of others. Seek permissions from anyone who appears in any photographs, video or other footage before sharing these via social media
  - **Do not** comment, contribute, create, forward, post, upload or share content that is malicious or defamatory. This includes statements which may negatively impact on the reputation of another
  - Always be courteous, and respectful of others’ opinions including detractors
  - Students must not use Artificial Intelligence tools to impersonate SWTAFE staff, representatives or official social media accounts.
  - Students must not create or share AI-generated content that is misleading, deceptive, defamatory or damaging to the reputation of SWTAFE, its staff or students.
  - The creation or distribution of synthetic images, audio or video (including “deepfakes”) depicting SWTAFE staff or students without consent is strictly prohibited.

9. Consequences if these Guidelines are breached

Staff and students who breach/ignore the Social Media Guideline will be considered to have breached the relevant Code of Conduct (staff or student) and disciplined in accordance with that Code.

Where the breach occurs outside of SWTAFE hours or on a private social media site, the incident will be assessed on an individual basis and monitored accordingly. When SWTAFE are aware of an incident that occurred off campus and/or out of hours, all efforts will be made to monitor the situation and put in place measures to ensure the safety and well-being of all staff and students.

In the event that external agencies or bodies are involved, i.e: police, welfare organisations and/or family members etc. SWTAFE will seek permission from all parties to ensure open communication regarding the situation.

10. Complaints Process

In the first instance, any concern with content on a SWTAFE Social Media platform should be raised with the Manager, Brand & Strategic Marketing.

Any formal complaints are lodged with the SWTAFE’s Audit, Risk and Compliance Officer who is the nominated complaints manager. They can be contacted in writing to:

Audit, Risk and Compliance Officer
South West TAFE
PO Box 674
WARRNAMBOOL 3280
Or via feedback@swtafe.edu.au
Or using the feedback button on the website: www.swtafe.edu.au/about-us/feedback/

11. Communication

These Social Media Guidelines are distributed to all students as part of the enrolment or course orientation process. It is also displayed in relevant student activity areas. It is also the responsibility of all staff to ensure that the Guidelines are regularly communicated and outlined to students.

12. Diversity, Equity and Inclusion

SWTAFE is committed to making diversity, equity and inclusion part of everything we do, including in the implementation of this policy/procedure/guideline. For more information, please visit the 'Our Values' page on our website [external] or the Diversity, Equity & Inclusion Homepage on ECHO [internal].
Diversity, Equity & Inclusion (DEI)

13. Statement of Commitment to Child Safety

South West TAFE is committed to the protection of all children from all forms of child abuse and demonstrates this commitment through the implementation of a Child Safe Program designed to keep children safe within our organisation. For Child Safe key documents, resources, contact officer details please go to: Child Safe Commitment

14. Use of Artificial Intelligence in Social Media

SWTAFE recognises that Artificial Intelligence tools may be used to support social media activities. AI may be used as an assistive tool only and must not replace human judgement, oversight or accountability.

All use of AI in social media must:

- align with SWTAFE values
- comply with privacy, security and information management obligations
- protect the reputation of the Organisation
- maintain trust with students, staff and the broader community

Where uncertainty exists regarding the appropriate use of AI, advice must be sought from the Manager, Brand and Strategic Marketing, ICT and/or the Risk & Compliance function prior to use.