

Section: External Relations (ER)**Subject:** Communications**Legislation:****Effective:** May 14, 2014**Revision:** September 1, 2016 (reformatted); June 19, 2019; September 23, 2019**APPROVED:** _____
President and CEO

POLICY

The policy of the Board of Governors is to ensure SAIT employees use social media in a responsible and professional way in order to build authentic engagement that supports SAIT's mission, goals, programs and priorities and at the same time protects SAIT's reputation.

PROCEDURE

DEFINITIONS

- Institutional account** A social media account that SAIT owns and that is dedicated to SAIT, a school, a department or a program. For example, SAIT School of Business on Facebook.
- Personal account** A personal account that SAIT employee owns.
- Primary administrator** The employee who holds the account credentials and has full administrative access to the account.
- Social media** A category of websites where users collaboratively generate the majority of content. It provides a model of communication in which a person or organization can have a conversation with many people at any one time. The tone of social media is conversational and is constantly evolving. Current platforms include but are not limited to:

The official controlled version of this document is held in the Board of Governors Office.

- a) Blogs and podcasts, including corporate blogs, personal blogs or blogs hosted by mainstream media outlets.
- b) Forums and discussion boards including comments or feedback sections of mainstream media websites.
- c) Microblogging sites such as Twitter.
- d) Professional networking sites such as LinkedIn.
- e) Social networking sites such as Facebook.
- f) Social news websites such as Reddit.
- g) Video and photo sharing sites such as Instagram, Flickr, Pinterest and YouTube.

GOVERNING PRINCIPLE

1. Employees who identify themselves as SAIT employees or reference SAIT in their social media use must follow SAIT's Social Media Guidelines.

PROCEDURE

A. Social Media Governance

1. SAIT empowers employees to responsibly use social media with the assistance and guidance of SAIT's social media team and communications team in the Communications department.
2. The Communications team coordinates social media efforts on behalf of SAIT. This includes managing, monitoring and measuring institutional accounts, and ensuring SAIT's Social Media Guidelines, attached as Schedule A, an Associated Document to this procedure, and the terms of service of each social media channel are followed.
3. The social media team provides training to SAIT. The team is also accountable for the institutional accounts, including managing, monitoring and measuring those accounts, and ensuring SAIT's Social Media Guidelines and the terms of service of each social media channel are followed. It is also accountable for managing the repurposing or decommissioning of accounts as necessary.

The official controlled version of this document is held in the Board of Governors Office.

4. Any account challenges or disputes that are not addressed by SAIT's policies and procedures, including procedure AC.3.4.1 Student Code of Conduct and procedure HR.4.10.1 Respectful Workplace and Learning Environment, will be escalated for resolution to the vice president, External Relations.

B. Creating New Accounts

1. Before an employee requests an institutional account, the employee must complete a checklist (available on SAITNOW) and submit it to the social media team for review and approval.
2. All account holders must provide full administrative access to all institutional accounts to the social media team, to be used in case of an emergency, security breach or employee departure.

C. Student Use of Institutional Accounts

1. When institutional accounts are designed primarily for student use (for example, an event), a permanent employee must be the primary administrator to ensure the account can be repurposed or decommissioned when it is no longer needed or relevant. For example:
 - a) On Facebook, the employee will be the 'manager' and the student(s) will be 'content creators'.
 - b) On Twitter, the employee will keep track of the log-in credentials, changing the password at the end of each term (before the outgoing students have left).
2. In a crisis or emergency situation, it is the employee's responsibility to ensure the account follows the proper emergency communications procedure. Refer to Section F of this procedure for more information.

D. Branding SAIT Accounts

1. All institutional accounts must:
 - a) Abide by branding criteria as outlined in SAIT's Brand Standards (available on SAITNOW).

The official controlled version of this document is held in the Board of Governors Office.



- b) Clearly identify themselves as an authorized communication channel of SAIT, and include 'SAIT' in the account name. For example, SAIT School of xxxxxxxx.
2. SAIT logos and/or visual identity cannot be used without permission. Details on when to appropriately use the SAIT logo are available in Schedule A, an Associated Document to this procedure.

E. Decommissioning Accounts

1. Social media channels that SAIT's social media team has identified as impacting or threatening SAIT's reputation by being inappropriately inactive, being redundant or having limited audience participation will be decommissioned or repurposed.
2. Before decommissioning an account, the primary administrator must consult SAIT's social media team.

F. Social Media Use during a Crisis or Emergency

1. In the event of a crisis, providing timely and accurate information to users is critical, and will be managed by Communications under the authority of SAIT's Emergency Management Response Team (EMRT).
2. Crisis-related social media communications will take priority on all SAIT accounts. An emergency or crisis includes but is not limited to an on-campus or off-campus incident that:
 - a) May be emotionally sensitive to students, employees, contractors and/or visitors of SAIT and other post-secondary institutions.
 - b) Puts the safety of students, employees, contractors and/or visitors at risk.
 - c) Damages or threatens to damage SAIT's reputation.
3. SAIT social media channels should not be used — other than to direct their followers to SAIT's institutional accounts and/or sait.ca — for crisis-related information and updates, unless the EMRT otherwise instructs.
4. All SAIT social media administrators must sign up for SAITALERT so they are immediately notified of an emergency. SAITALERT is available for download from the iOS and Android app stores.

The official controlled version of this document is held in the Board of Governors Office.



5. In the event of a reputational emergency, SAIT social media administrators will be notified with further instructions. In the case of a reputational issue relating to an institutional account, administrators must immediately notify the SAIT social media team.

G. Security

1. At least one permanent SAIT employee must have administration access to every institutional account.
2. Third party administrators, such as contractors or students, must be immediately removed from the accounts once access is no longer required.
3. Best practices must be followed regarding password protection, as per procedure AD.2.10.1 Password Procedure. See also Schedule A, an Associated Document to this procedure.

ASSOCIATED DOCUMENTS

Schedule A Social Media Guidelines

POLICY/PROCEDURE REFERENCE

ER.2.1 Social Media Use policy

The official controlled version of this document is held in the Board of Governors Office.