1. Introduction

Social media platforms offer opportunities for the De La Salle-College of Saint Benilde ("College") and members of the community to communicate, to use for teaching and learning, and to engage a wide range of audiences and stakeholders. It likewise provides professional and personal opportunities for associates and students. However, there are also a number of risks associated with the use of social media which can have a negative impact on the College's reputation. Thus, this policy provides guidance to associates and students on how to safely and productively use social media to maximize the range of benefits it offers but at same time mitigate the risks associated with it. This also provides the following information: on responsibilities of associates and students and other groups affiliated with the College when communicating via college social media accounts; expectations from associates on their individual, personal and professional accounts; and expectations of students in relation to the use of their social media accounts. This policy respects the individual's right to freedom of expression and is not a form of censorship.

2. Objectives

2.1 To provide associates and students with information on College requirements and expectations regarding use of social media platforms in both professional and personal capacity;
2.2 To ensure a consistent approach to social media usage across the College;
2.3 To be informed of and to mitigate the risks associated with social media in order to protect associates, students, and the College;
2.4 To ensure associates and students do not compromise their personal security or the security of College information assets;
2.5 To define the responsibilities of users of College social media accounts; and
2.6 To outline channels for addressing issues or concerns

3. Definition of Terms

Social media are websites and applications that enable users to create and share content or to participate in social networking.

- Examples of which include, but are not limited to:• Twitter • Facebook • YouTube • Instagram • Snapchat • WhatsApp • LinkedIn • Flickr • Messenger • Reddit • Pinterest • Wikis and blogs/vlogs

4. Scope

This policy applies to social media communications made both on public and private forums by DLS-CSB associates, students and other groups affiliated with the College. Posts added to public forums can be viewed by the public from date of publication but posts added to private forums can also be shared publicly by others.

5. Guideline Statements

5.1 Use of Social Media Platforms

5.1.1 Associates and students using social media should be mindful of the following legal risks and acts in particular:

5.1.1.1. Libel: Public and malicious imputation of a crime, vice or defect, real or imaginary, or any act, omission, condition, status or circumstance tending to cause dishonor, discredit or contempt of a natural or juridical person, or to blacken the memory of one who is dead (Art. 353, Revised Penal Code and Cyber Crime Law)

5.1.1.2. Harassment: subjecting someone to a course of conduct that causes them distress or alarm, including stalking, trolling and cyber-bullying (refer to DLS-CSB Associate/Student Handbook)

5.1.1.3. Intellectual property infringement: posting content which copies a substantial part of a work protected by copyright (refer to DLS-CSB Intellectual Property Policy)

5.1.1.4. Data Privacy infringement: posting personal information of others without their consent (refer to DLS-CSB Data Privacy Policy/Manual)

5.1.1.5. Breach of confidence: unauthorized posting of confidential information

5.1.2 Students and associates must familiarize themselves with the confidentiality rules of the College and other laws but not limited to the following:

- Cybercrime Law of 2012 (RA 10175)
- Data Privacy Act of 2012 (RA 10173)
- Intellectual Property Code (RA 8293)

5.1.3 Other relevant policies and guidelines of the College that are applicable to social media accounts are: Information Security Policy, Data Privacy Policy, Associate and Student Conduct and Discipline as found in the Associate/Student Manual.

5.1.4 This policy shall form part of the College's contractual requirements with the associates and the students as may be found in their respective manuals.

5.1.5 **Appropriate use**

5.1.5.1 Associates may make reasonable and appropriate use of social media from DLS-CSB and personal devices. Time spent on social media during working hours should not interfere with their duties. The Head of the department or units shall be responsible for monitoring their subordinates' use of social media during work hours.

5.1.5.2 Associates and students should be mindful of how their statements, views or posts appear on line. They are reminded that the public, future employers, industry contacts and other College stakeholders may view their posts and these may have a negative impact on their reputation, reputation of others and reputation of the College. They must also be aware of the permanence of anything posted on line.

5.1.5.3 There are proper venues for any complaints or disclosure of malpractice, wrongdoing, impropriety involving the College and the members of the College community. These can be directed to the proper office as the case may be. An associate/student should not release such complaint/information through social media.

5.1.6 **Individuals' personal and professional accounts**

5.1.6.1 It is recommended that official DLS-CSB Social media platforms shall be the venue of College announcements.

5.1.6.2 If associates post on their personal social media accounts, it is understood that the views expressed are their own and do not necessarily reflect those of the College.

5.1.6.3 All associates and students should consider what they are posting on their individual accounts. The College do not actively monitor individual associates' or students' social media accounts. However, if a concern is raised regarding content posted on associate's or student's social media account and the post is considered to be a violation as provided in Section 5.1.1 or affecting the good reputation of the College, the College has, through its representatives, the right to request or require, as the case may be, the removal of inappropriate content. In addition, the matter may be addressed through the College's Disciplinary Procedure. Serious breaches may constitute serious misconduct and may be a ground for appropriate disciplinary action. If any member of the community notices, or is made aware of, social media

activity of an associate or student which raises concerns or constitutes a violation, they have obligation to alert by emailing or calling the Human Resource Services or Office of Student Behavior, as the case may be.

5.2 DLS-CSB Social Media Accounts

5.2.1 **Setting up a new official DLS-CSB social media account**

5.2.1.1 Before creating a new DLS-CSB social media account:

5.2.1.1.1 Associate/unit/department should consider whether there is a different audience or set of objectives which cannot be met through an existing DLS-CSB social media account

5.2.1.1.2 A proposal for approval should be submitted to the Branding and Communication Advancement (BCA). Proposal shall include the target audience and their information needs; the content to be shared; how producing content and monitoring the account will be resourced; and how this account sits together with those already established across the College.

5.2.1.1.3 If after approval, a new account is to be established, it should follow the Benilde style guide for consistency with other College social media accounts.

5.2.1.1.4 The new account and person-in-charge must be registered centrally with BCA.

5.2.2 For departments/units with existing social media accounts, they shall register with the BCA within the prescribed period. BCA shall call the attention of unofficial sites that it cannot use the brand name, logos and copyrighted thematic lines of Benilde. Accounts which are not registered shall be reported as unofficial by BCA subject to the action of the social media platform.

5.2.3 BCA shall maintain an asset register of all DLS-CSB social media accounts with a designated account owner. This is important for emergency situations and to keep associates/students across the institution up to date with policy changes and training opportunities.

5.2.4 Any DLS-CSB social media account that violates this policy may be subject to cancellation of its registration in the BCA.

5.3 **Social media account management: All DLS-CSB registered social media accounts must adhere to the following:**

5.3.1 College's style guide and the account profile information should clearly state the purpose of the account and the hours during which it is monitored.

5.3.2 All social media accounts are kept up to date and regularly monitored. Questions raised in the social media platform should be responded to promptly within operating hours.

5.3.3 Where several persons have access to the same social media account, there must be an agreed point person.

5.4 **Social media posts**

All posts from DLS-CSB social media accounts represent the College. It is vital that due diligence is observed at all time in posting messages posted. Ensure that messages must be appropriate and ensure that no damage to the reputation of the College committed.

5.4.1 Safeguards should be put in place to minimize the risk of communication errors via social media, including checking veracity or due authenticity of content(s) before publishing.

5.4.2 Posts must be in line with the values and ethics of the DLS-CSB and all relevant college policies, including Regulations for the Use of IT Services.

5.4.3 Those posting content on DLS-CSB social media accounts must not post or promote content:

5.4.3.1 Which harasses, bullies or otherwise intimidates;

5.4.3.2 Which instructs, causes or coerces others to harass, bully or otherwise intimidate;

5.4.3.3 Intended to incite violence or hatred;

5.4.3.4 Abusive content relating to an individual's age, disability, gender, civil or social status, race, religion or belief, sex or sexual orientation or political belief; and

5.4.3.5 Inappropriate images, photos, videos, and audio recordings unbecoming of a Benildean-Lasallian associate/student.

5.4.4 Content posted or promoted on the College social media accounts must at all times be respectful of others and courteous.

5.4.5 Social media accounts must not be used to criticize or argue with colleagues, students, parents, clients, partners, stakeholder or competitors.

5.4.6 When posting on an account, it is vital to keep the legal ramifications in mind. This includes, but is not limited to, ensuring that posts do not breach confidentiality, make defamatory comments or breach copyright.

5.5 **Communications through social media must not:**

5.5.1 Discuss the College's internal workings or reveal future plans that have not been communicated to the public;

5.5.2 Reveal intellectual property;

5.5.3 Disclose personal information; and

5.5.4 Breach the professionalism and confidentiality rules of College.

5.7 It is also important that content is accurate and does not commit to something which the College does not intend to deliver. If a mistake is made, it is important to be transparent and update the page with a correction. Person-in-charge shall be responsible that he/she exercised due diligence in double checking accuracy of information before posting. For posts with grave mistakes or erroneous statements, this may mean being subject to disciplinary action on the person responsible for such post/s.

5.8 Accessibility

5.8.1 All film content which is externally produced or produced in advance for use in a social media campaign is recommended to have subtitles for accessibility purposes.

5.8.2 It is accepted that some film content for social media is either live streamed or produced for immediate use officially by the College (given the immediacy of the channel), however the BCA shall be informed of such live streaming.

5.9 Account security

5.9.1 Social media accounts are at risk of hacking and this can cause significant reputational damage and potentially serious misinformation for stakeholders. There are also considerable resource implications resulting from any breach in security such as a compromised social media account. Where associates require access to the same social media account, there must be an agreed overall person-in-charge.

5.9.2 It is recommended that the person-in-charge choose a strong and secure password which are different from personal passwords and in line with password guidance provided by Data Technology Office (DTO).

5.9.3 The person-in charge is responsible for maintaining a full log of staff with access to the account's password and the password must be changed whenever one of those staff members moves on to a different role or different institution.

5.9.4 In cases of emergency, such as hacking of a DLS-CSB social media account, the BCA may need to urgently address this concern beyond office hours thus must have direct access to the person-in-charge of the social media account.

5.9.5 Where persons-in-charge are accessing the DLS-CSB social media accounts on mobile devices, if device is lost or compromised it should be reported to the DTO.

5.10 Addressing social media accounts concerns and issues

5.10.1 If a DLS-CSB social media account has been hacked or compromised or attracts a number of negative comments and it is not clear how best to respond, person-in-charge should flag this with BCA and seek guidance.

5.10.2 When the issue is considered serious and damaging to DLS-CSB's reputation, the Crisis Management Team shall be constituted in accordance with the College's Crisis Management Plan.

5.11 Social media in an emergency

5.11.1 Social media provides important information channels for associates, students and stakeholders during an emergency situation and it is vital that the information provided is timely, consistent and accurate. All communications on social media from the College in an emergency situation will be issued only through the College's official social media account/s.

5.11.2 Any suspension of classes shall be announced by the BCA in coordination with the related offices, though the College email system, College intranet WeBenilde, and social media via the official Facebook and Twitter pages.

5.11.3 In order to minimize the risk of issuing conflicting and/or incorrect information, it is vital that all other social media accounts do not post information or updates during a live incident.

5.11.4 Misuse of Official Social Media Accounts by associates and students may be subject to disciplinary sanctions in accordance with the College rules and regulations.

REFERENCES

LAWS:

Republic Act No. 8293, Intellectual Property Code of the Philippines
Republic Act 10173, Data Privacy Act of 2012
Republic Act No. 10175, Cybercrime Prevention Act of 2012
Act No. 315, Revised Penal Code of the Philippines

URL GENERAL WEBSITE ARTICLE WITHOUT AUTHOR

The University of Liverpool. The University of Liverpool Social Media Compliance Policy. Retrieved from: https://www.liverpool.ac.uk/media/livacuk/computingservices/regulations/social-media-policy.pdf