CIU Columbia International University

Policy Number	710.000
Policy Title	Social Media Policy
Responsible Officers	Director of University Communications
Responsible Offices	University Communications
Summary	Social media is a means through which CIU can communicate with a worldwide audience for the purposes of recruitment and advancement. More than that, it reaches people with the message of Christ. The purpose of this policy is to create a clear system of how to establish official University accounts, what responsibilities come with maintaining these accounts, and how to keep the accounts secure.
Definitions	• Account Administrator – A University staff member within a department charged with communications oversight at the departmental level. • Account Manager – A CIU faculty member, staff member or student who administers or authors content for any University social media account. • Department – A college, school, office, team, club or any other operating CIU-affiliated group. • Social Media – A website or application that enables users to create and share content or to participate in social networking. Various platforms include (but are not limited to) Facebook, Instagram, X (formerly known as Twitter), Snapchat, TikTok, YouTube, and other websites with user-generated content. • User – A person who places postings, comments or other content on a University social media account or space.
Approving Body	Academic Council; Administrative Council
Approval Date	710.000 Aca C (06.10.2024); Admin C (05.22.2024)
Last Revision	May 2024
Re-evaluation Date	Fall 2027
Departmental Impact	Faculty, Staff, Students who manage CIU-affiliated social media accounts

Failure to follow the following policy may result in disciplinary action, including termination of employment.

Policy Statement

Columbia International University recognizes the value of social media as a powerful tool for communication and conversation with a global audience for the purposes of recruitment, recognition and public relations. As various social media channels are speaking on behalf of the University yet managed by multiple people from multiple departments, it is important to maintain clear authorization and security of each channel and to promote and protect CIU's brand identity, integrity and reputation.

Rationale

This policy provides directions on how to register or establish official University social media accounts and how to maintain the ownership and security of those accounts. The department of University Communications, being responsible to define CIU's branding identity, maintain positive public relations, communicate effectively with CIU's audiences and manage major and crisis communications, will therefore supervise all University social media communication channels.

It is CIU's desire that each approved social media account can showcase the many facets of the University and be a successful tool in supporting the goals of recruitment, recognition and positive public relations.

Policy Procedures

Social Media Account Registration & Application

Accounts created on or before June 1, 2024, must register with University Communications by July 1, 2024. After July 2024, social media account administrators must apply to create new accounts with University Communications and proceed only once approval is received. The purpose of this is to keep an updated directory of accounts and to allow for periodic quality control checks to occur.

Account registration requires:

- Full account name
- Two best contacts (CIU employees) with email addresses
- Justification that the account will support CIU's mission and goals
- Strategy to create and maintain content
- Acknowledgement to notify University Communications when changes are made to account administrators

Existing account approval form New account request form

Account Administrator Responsibilities

- Work collaboratively with University Communications to review social media accounts to ensure the accounts remain active, meet the branding guidelines and engage with their audiences.
- Provide guidance and support for new account administrators or, if needed, seek guidance from University Communications.
- Transfer access to another social media manager for University social media accounts, as appropriate, when University employee or student status changes.
- Terminate any university social media accounts that cannot be made compliant with this policy.
- Terminate obsolete accounts.
- Notify University Communications of any changes in account status (inactive, deleted, etc.) or Administrators/ Managers.
- All of the above plus Account Manager responsibilities listed below.

Account Manager Responsibilities

- Consult the CIU Social Media Marketing Toolbox and/or consult with your communications professional for guidance before launching a social media account or if you are registering an existing account. Both new and existing accounts will need to submit a reason for the account, a strategy for creating and maintaining content and comments, and note what positions will be responsible for the account.
- Follow university branding guidelines.
- Take action if it is suspected that their accounts have been hacked or compromised. This should include changing passwords, informing supervisors, and monitoring for suspicious activity.
- Monitor comments and engage with users (see Rules of Engagement).
- Correct or modify university social media accounts as directed by University Communications when necessary.
- Refrain from using or posting to University social media accounts in a manner that is in violation of this policy.
- Be aware of each platform's policies and guidelines.
- Be aware of ADA compliance standards regarding social media, specifically regarding including Alt Text (image description) on every photo posted. (Use this guide for Alt Text assistance.)

University Communications Responsibilities:

- Oversee CIU's institutional presence on social media platforms.
- Review applications to create social media accounts on new platforms as they become available. Authorize these accounts as appropriate.
- Review social media accounts that represent the University for compliance with this policy.

- Instruct account administrators to correct, modify, or terminate University social media accounts that are not in compliance with this policy.
- Advise on responding to complaints and comments as the need arises.
- Make branding assets and style guide available to account administrators via an online Marketing Toolbox.

Major Announcements and Crisis Communications

- When a major announcement is made from the University, University Communications will send appropriate graphics and/or photos and copy to post on all platforms (or major platforms). These should not be altered before posting.
- When experiencing a crisis situation, University Communications will work with the Vice President of Institutional Advancement and the President's Office to create appropriate messaging. This keeps a clear line of communication to CIU's many audiences.

Direct Messages

- Direct messages (DMs) sent through an approved, official CIU social media channel serves as a communication on behalf of Columbia International University
- DMs must not violate the "Prohibited Use" section of this policy.
- DMs do not offer the same privacy as an @ciu.edu email account, as each social media channel will be accessible to more than one person.

Rules of Engagement

When writing on behalf of the University (in posts, comments or DMs), please do so in CIU's brand voice.

Proactive engagement:

- When possible, respond to others' comments; this builds community and reaches a larger audience.
- When possible, engage on other accounts involved with CIU (ex: @ciuramssoftball commenting on a player's post about the team); this builds community and reaches a larger audience.

"Negative" comments or DMs - defined as any negative words that are not "Unwanted" or "Harassing" (see below):

- If the comment is in context to the conversation, allow the comment to remain. CIU does not need to reply. Often, others will add comments and a healthy dialogue occurs.
- If the comment is wrong or inaccurate, correct the commentor quickly, publicly and with kindness.

"Unwanted" comments or DMs - defined as: spam; confidential information; defaming language; degrading language:

- Take screenshots of the comments, noting the date and timestamp
- Send screenshots to the Strategic Communications Manager or Director of University Communications
- Hide comments from public view

"Harassing" comments or DMs - defined as: obscene or threatening language, photos or graphics; encourages illegal or unlawful activity:

- Take screenshots of the comments, noting the date and timestamp
- Send screenshots to the Strategic Communications Manager or Director of University Communications
- Hide comments from public view

Acceptable use of information systems at CIU

- Access to CIU owned or operated computer systems and networks imposes certain responsibilities and is subject to University policies, and local, state and federal laws.
- Social media account administrators are required to be familiar with CIU's Acceptable Use Policy.

Account Security and Passwords

- At least two people should have access to every social media account. At least one of them should be a CIU employee.
- All social media channels will be linked to a shared departmental @ciu.edu email address.
- Joint owners of any one shared departmental @ciu.edu email address cannot be related to each other, unless another non-familial CIU employee shares the same email address.
- Use account management tools provided by platforms, when possible. Ex: Meta Business Suite offers resources for managing access and keeping personal and business accounts separate.
- All Facebook accounts should be "owned by" Columbia International University. Once your account is approved and created, the CIU Facebook page will send the approved account a request to be claimed by CIU.
- Only people who are currently managing the account should have the current password. Change passwords as quickly as possible each time someone who has access leaves or changes roles and no longer needs access to the account.
- New passwords should be securely shared - either over the phone or in-person. No passwords should be shared via email.
- All communications professionals and account administrators must remain compliant with CIU's Password Policy.
- Student takeovers must follow University Communications Student Takeover Guidelines.

Prohibited Use

The following are prohibited when posting or commenting as a University social media account (on behalf of the University):

- Illegal or unlawful activity
- Violations of University policies
- Sharing account passwords with individuals not authorized to manage accounts
- Publication of confidential, financial, legal or non-public operational information
- Endorsing political candidates or views
- Defamation, derogatory statements, obscene language, or threatening language

Personal Social Media Accounts of University Employees

This policy does not seek to limit personal use of social media by faculty, staff, or students. Personal social media accounts may list University affiliation in the bio or about sections. Use of University brand elements on those accounts in ways that violate branding guidelines or other University policies is prohibited. Note that, even on personal social media, faculty, staff and students should be mindful that they are still being seen as a representative of their college/school, department or the overall University.

Hyperlinks

www.ciu.edu/policy