

NC DIT Social Media Policy

Updated: February 2018

Purpose

To provide guidelines for employees of the Department of Information Technology in using social media to communicate with the public, while maintaining the mission and vision of the department. Adherence to this policy is mandatory, and all compliance should be completed by [DATE].

Owner

Legislative and Public Affairs

Policy

- I. Definitions
 - a. Social Media: websites and applications that allow users to create and share content and to network. Examples include, but are not limited to:
 - i. Micromedia: Twitter, Facebook, LinkedIn
 - ii. Video: YouTube, Snapchat, Facebook Live, Periscope
 - iii. Photo Sharing: Instagram, Flickr
 - iv. Messaging: Skype, Slack
 - v. Survey/Scheduling: Survey Monkey, Doodle
 - vi. Blogs
 - vii. Podcasts
 - b. Social Media Account: The account and account name registered on a third party social media site or platform.
 - c. Worker: Any employee, Full-time (permanent, probationary, or time-limited), Part-time (permanent, probationary, or time-limited), probationary, temporary, contractor or intern working for DIT.
- II. Official Use of Social Media
 - a. It is the responsibility of DIT employees in control of any department account and any employees in control of DIT division accounts to understand and adhere to this policy. Employees should use reasonable judgement in creating and using social media accounts and applications, and any questions regarding such should be directed to the DIT social media manager or the Director of Legislative and Public Affairs. Any worker who does not follow this policy may be subject to disciplinary action, up to and including dismissal.
 - b. Process
 - i. Approval: Employees or divisions considering the use of any social media platform for an agency account should make sure the platform aligns with the mission and vision of DIT. Such platforms must be approved by the Director of Legislative and Public Affairs and the Secretary of DIT.
 - ii. Registration: All account names must relate to the agency or office of DIT and should be set up using an official State email address. If possible, account names should be consistent across all platforms to reduce confusion and improve search optimization, and should include "NC" to denote a State account. The account must state that it is an official account of the Department and that all content and communication is subject to N.C. Public Record Law. Profile images shall include the logo of the department and



- iii. header images shall have the name of the department in the corner. All accounts need to be registered with the State Archives Office.
 - iv. Followers: Accounts followed by DIT should be relevant to the mission of the agency and should be bipartisan. Users of official State accounts should not follow political campaign accounts.
 - v. Content: Employees should carefully consider any content posted, as such content could be perceived as an official DIT or State of North Carolina position, comment, or statement. It is important for each account to remain neutral. Confidentiality should be protected at all times; ask for permission to post content. Copyright laws must be followed; when referencing someone else's work, a citation or link to the original work must be provided.
 - 1. Photos: Take care when posting other users' photos. Make sure proper credit is given to the creator or account and that there are photo releases in instances when children are in photos. Confidentiality should be protected at all times; ask for permission to post on social media, and be aware of what information can be seen in the background of photos.
 - 2. Gifs: [need department stance]
 - 3. Infographics/Graphics: Any graphics posted should include the NC DIT logo in the corner of the graphic and follow the guidelines in the Style Guide.
 - vi. Replies: The department's Rules of Engagement should be followed. [see section...]
 - vii. Monitoring: Time should be devoted each day to monitoring each social media account for comments, replies, tagging from other accounts, trolls, and trending topics.
 - viii. Audits: Audits of social media accounts should be performed on a regular basis. This includes monitoring followers for fake accounts and bots and running an analysis for engagement and clicks.
- c. Accuracy
- i. Review content before posting to make sure facts are correct. Review content for spelling and grammar errors; any errors reflect badly on DIT and the State of North Carolina.

III. Personal use of Social Media

- a. Excessive personal use of social media by State of NC staff during work hours is prohibited. Incidental personal use of social media while at work (*e.g.*, providing personal updates to a Facebook page or Twitter account during work hours), when such activity is outside of the employee's official job function, shall not interfere with employee's work responsibilities.
- b. Personal use of social media outside of work is subject to First Amendment protections. Where such personal use is related to subject matter pertinent to State employment, it must be conducted in such a manner that no impression is created that the employee is speaking on behalf of the State. For example, employees may put a disclaimer in their social media profile indicating that expressed opinions do not reflect that of the State or DIT.
- c. An individual's social media identity must be distinct from the State and agency usage identity, for instance, established under a personal email account, and not a State email account.
- d. If an employee identifies himself or herself as a State employee or the employee's personal expression suggests that the employee is an employee of the State, the employee should include a clear disclaimer indicating that the employee is not communicating on behalf of the State.
- e. Employees must refrain from disclosing Restricted or Highly Restricted State of NC information.



- f. Employees are prohibited from using State-issued e-mail addresses for any personal social media account.

IV. Rules of Engagement

- a. Users have First Amendment rights, and users' comments or speech cannot be removed for expressing disagreeing viewpoints with the agency. Comments may only be removed if they are obscene, threatening, discriminatory, or harassing.
- b. Comments and posts should be moderated in case of discussions going off-topic or if they are obscene, threatening, discriminatory, or harassing.
- c. All posts and comments, whether from agency employees or the public, are subject to North Carolina Public Records Law.
- d. Topics, comments, responses and posts that are negative and should be avoided include:
 - i. Conduct not acceptable in the workplace such as harassment, ethnic slurs, personal insults, or obscenity.
 - ii. Controversial topics such as party politics, religion, race, and ethnicity.
 - iii. Disputes between State agency employees.
- e. Transparency should be maintained at all times. If a post needs to be altered, an indication should be made. Any mistakes should be corrected immediately.
- f. Social media accounts can be used to clear any misrepresentations in the media as long as facts are accurate and correct.

V. Cybersecurity

- a. Passwords for social media accounts should be a phrase or sentence that contains at least 12 characters.
- b. Each social media account should have a different password.
- c. When available, enable two-step verification.

VI. Crisis Communications

- a. In the event of a crisis, close contact must be maintained with the Director of Legislative and Public Affairs, the Secretary, and any other designated staff. The department's Crisis Communications Plan should be followed.

VII. Best Practices

- a. Business Strategy
 - i. Goals for each social media platform should be established and reviewed as needed.
- b. Risk Assessment
 - i. A cost-benefit analysis should be performed to determine which social media platforms would be beneficial to DIT's mission and vision.
- c. Correct Account Checks
 - i. If posting from a mobile device, take care to make sure you are posting to the right account. If a personal tweet, post, or comment is posted on a DIT account, protocol in the Crisis Communications plan should be followed.
- d. Accuracy
 - i. Ensure that all facts and information posted to social media are correct.
 - ii. Check for spelling and grammar mistakes and for correct punctuation.
 - iii. Check that any and all accounts tagged or mentioned in social media posts belong to the right person or organization.



- e. Respect
 - i. All social media posts reflect not only on DIT as an agency, its staff, and its leadership, but on the State of North Carolina as a whole.
 - ii. Ensure that posted content will not alienate, harm, or provoke.
- f. Neutrality
 - i. Posts should remain nonpartisan and free from the appearance of promotion or endorsement of businesses and candidates.
- g. Rules of Engagement
 - i. Please see section IV for complete Rules of Engagement.
- h. Code of Ethics
 - i. Social media engagement should follow the state's Ethics Law, where applicable.
 - ii. The content should be truthful and provide the audience with correct and sufficient information.
 - iii. DIT's publics, audiences, and stakeholders should be respected. Content should not discriminate, treating everyone as human beings no matter their race, color, sex, age or ethnic origin.
 - iv. Transparency should be maintained at all times.
- i. Press Inquiries
 - i. All press inquiries should be routed through the Director of Legislative and Public Affairs and other designated staff as needed.