

Social Media Guidelines



Account Owner Contact and Sign-Up Information

Account Contact Information

In order to make social media account creation, management, and continuity an easier and more secure process, we ask that the following guidelines be followed.

Never use personal or individual email accounts or phone numbers for a unit's social media account(s). Using a departmental email address, [socialmedia@\[department.rutgers.edu\]](mailto:socialmedia@[department.rutgers.edu]) for example, and phone number ensures that, if the person managing the account leaves, the account can still be reset in case the password is lost.

Before Creating a New Social Media Account

Before creating a new account, follow these steps:

1. Review the Rutgers Social Media Playbook
2. Decide if social media is the correct tool for your unit
3. Develop a plan for how this account will be used in the context of your unit's overall marketing and communications strategy
4. Reach out to the [assistant director of social media strategy, University Communications and Marketing](#), if you have questions and to alert them to your plan to launch a new social media channel

Page Roles

We suggest that all units establish page roles for all members who will be accessing the page. Some social media channels and social media management tools, like Hootsuite or Sprout Social, have predetermined user or page roles that can be used to control who has the power to manage or post to the channels.

If you have questions about establishing page roles, contact the [assistant director of social media strategy, University Communications and Marketing](#).

Continuity Plan and Approval Authority

In addition to developing page roles, it is important to develop a continuity plan, establish levels of reviews, and determine who has top-level approval authority.

A continuity plan will help with succession when people who have access to the account(s) leave the unit. Consider who will take over the account when the main operator leaves or how responsibilities get transferred when student managers graduate. Put this plan in writing and share it with the appropriate members of your team and your unit's leadership.

In day-to-day posting, it is helpful to develop a system of reviewing posts to ensure quality and accuracy. These levels of review will also be helpful when approaching and responding to comments and messages sent to the page. Additionally, determine who has final approval authority in case of the need to respond to emergency situations or other sensitive matters via social media.

Access List

For the unit's records, keep an updated list of all personnel who have access to the social media accounts at all times. This list should show which personnel have access as well as their role for each account.

Rutgers Social Media Guidelines

Statement of Use

In the About section of your Facebook page, and any other applicable accounts, consider including a statement of use. This statement of use sets the ground rules for individuals posting content or replies to your page and allows the unit to set stipulations for what kind of posts will be removed from the page if necessary.

Example:

We want you to share information, ideas, and opinions on this page, but we reserve the right to remove posts containing profanity, personal attacks, commercial promotions, political campaign materials, irrelevant information, or posts otherwise deemed to be inappropriate. The comments posted by followers of this page reflect the opinions of the individual poster and do not reflect the views of Rutgers, The State University of New Jersey.

Statement of Confidentiality Agreement

It is recommended that student personnel who will be managing social media accounts for your unit sign a statement of confidentiality agreement. You can use [the agreement available through the Rutgers Office of Student Employment](#) and amend as necessary.

Security

With the growing risk of cyberattacks and account hacking, the following social media security guidelines have been created to help mitigate avoidable incidences of account compromise.

Passwords

Passwords are the first line of defense in protecting social media accounts. In many cases, account administrators have been using the same passwords far longer than they should, and many of them are far too simple.

Passwords must be changed at the end of every semester or when someone who has access to the password leaves.

Passwords should follow the same policy as the Office of Information Technology's policy for NetID passwords:

- Your password/passphrase must be at least 10 but no more than 63 characters.
- Your password must contain a minimum of 3 character classes. These classes are:
 - Lowercase letters (a–z)
 - Uppercase letters (A–Z)
 - Numerals (0–9)
 - Special characters (e.g. \$ *)
- Spaces, tabs, and carriage returns are not allowed.

If possible, passwords should not be shared with anyone via electronic communications methods. Whenever passwords need to be exchanged, do so in person or over the phone. Additionally, avoid storing passwords online or on shared drives.

For more information on developing secure passwords, review the OIT Information Security Office's password guidelines: <https://rusecure.rutgers.edu/passwords>

Branding, Content, and Posting

Account Name, Profile Pictures, and Cover Photos

When choosing the name for the unit's page, profile picture, and cover photo, follow [university branding and visual identity standards](#). The social media page should clearly identify that your unit is a part of Rutgers University, so "Rutgers" must be included in the page name.

Rutgers Social Media Guidelines

Use High-Quality Visual Content

Use high-quality photo, video, and design content on your unit's social media pages. The page reflects Rutgers, The State University of New Jersey, and as such the content should be finely curated and of the highest quality. If you need help capturing high-quality photos, creating videos, or designing quality visual content, consult the communications office for your department, division, or chancellor-led unit, or contact the experts at [University Communications and Marketing](#).

Posting Guidelines

- Use proper grammar, spelling, and punctuation. Review the [Rutgers Editorial Style Guide](#) for assistance with style and the use of inclusive language.
 - Do not use vulgar language or profanity.
 - Do not share information that is confidential, proprietary, or not public.
 - Do not plagiarize or steal visual content. When sharing content from another creator, obtain permission and credit the source.
-

Community Engagement

Social media by its nature allows members of the community to come together to share ideas, thoughts, and concerns. While these interactions usually will be positive, in some cases the comments and interactions community members have with your account may be negative or even inappropriate. In most cases, refrain from deleting these comments. For negative comments, assess if it is possible to respond to the poster in a way that would alleviate the issue they are having and, if possible, take the conversation off social media.

Statement of Use

Set the tone for the unit's social media sites with a statement of use. This statement should reflect the unit's overall approach and let your audience know what kind of content and feedback is acceptable. If possible, it should be displayed in a prominent location on all the unit's social media sites. This statement will serve as a guide for account administrators when determining how to respond to feedback and what user content should be removed, where applicable. Make sure all administrators, including any student administrators, understand the policy and are comfortable using it.

Example:

We want you to share information, ideas, and opinions on this page, but we reserve the right to remove posts containing profanity, personal attacks, commercial promotions, political campaign materials, irrelevant information, or posts otherwise deemed to be inappropriate. The comments posted by followers of this page reflect the opinions of the individual poster and do not reflect the views of Rutgers, The State University of New Jersey.

Inappropriate Comments

In cases where inappropriate comments are made on posts, first assess if it falls into the category of unprotected speech. Types of speech that fall into this category include true threats, blackmail, defamation, obscenity, child pornography, fighting words, solicitations to commit a crime, incitement of imminent lawless action, perjury, and plagiarism. If the content in question falls into one of these categories, report the content using the tools provided by the platform it is posted on. This action will usually result in the content automatically being hidden or deleted depending on the platform.

For post spammers, those who copy and paste the same message on various posts, some social media platforms will automatically detect this behavior and hide or delete this content for you; however, if they miss these posts, report these posts as spam.

If a post or message contains a direct threat of violence against an individual or group, take a screenshot of the material, hide it from other followers of your page, and report the post/message to RUPD for investigation. Make sure you do not delete these messages or posts in case they are needed for investigation.

Rutgers Social Media Guidelines

Assessment

Perform an assessment of the unit's account activity at regular intervals. Focus your assessment on:

- The net change in followers/subscribers/likes for your unit's account(s)
- The number of impressions the account has or the account's total reach
- The number of engagements your posts have had
- The most popular posts
- The least popular posts
- Consider what social media ads were created or what posts were promoted
- Any surprising occurrences of note on the account?

Use this assessment when reviewing what content was effective for the account(s) and how to better plan content and use social media in the future. If you have more questions about assessing the performance of your account(s), contact the [assistant director of social media strategy, University Communications and Marketing](#).

Conduct on Personal Social Media Accounts

Faculty, staff, and students should be aware of how they identify and present themselves to the public via their own social media accounts as they may be seen as de facto Rutgers authorities.

If you distribute or comment on information related to Rutgers via personal accounts, it's important for you to clarify whether you are doing so in an official capacity or as a private individual. Make it clear that your personal comments represent your own viewpoints and not those of the university or its administrators. Keep in mind that your social media conduct may be copied or distributed by others long after you post it. You may be held liable for published information or find that it is used against you in an employment situation. Faculty and staff should also follow all applicable university policies, including but not limited to those addressing student and patient privacy, when conducting their own activities on social media.

Related Rutgers Policies

Social media administrators should follow all applicable university policies when posting and responding to content on Rutgers' social media accounts, including but not limited to:

- 70.1.1 Acceptable Use Policy for Information Technology Resources
- 80.1.2 Rutgers University Trademark Management and Licensing Policy
- 80.1.3 Purchase of External Advertising
- 80.1.4 Endorsements, Sponsorships, and Advertising in and on University Assets and Communication Materials
- 80.1.5 University Visual Identity
- 80.1.6 Communication and Relations with the News Media

Policies can be found in the [Rutgers University Policy Library](#).