

Applies to: Faculty, staff, student-employees, and other individuals who create and/or maintain institutional social media accounts for official university marketing or communications purposes.

INSTITUTIONAL SOCIAL MEDIA ACCOUNT PROTOCOLS AND STANDARDS (ISMAPS)

The Institutional Social Media Account Protocols and Standards support the implementation of the university's Institutional Social Media Account for Marketing and Communications Purposes policy. The procedures and guidance set forth in this document are designed to (1) support the use of social media to raise university brand awareness, engage audiences, drive action, and spur advocacy in support of the university's teaching, research, and service missions, the university's administrative functions, and students' campus-life activities; and (2) help ensure that Ohio State consistently protects its security, brand, and reputation, and satisfies legal, regulatory, and contractual requirements.

All institutional social media accounts for marketing and communications purposes are expected to be managed in a way that complies with the ISMAPS.

Table of Contents

| | |
|----------------------------------------------------|----|
| Social Media Application..... | 1 |
| Social Media Accounts – Minimum Requirements | 4 |
| Primary Account Criteria and Management..... | 5 |
| Account Takeover Standard | 6 |
| Account Recovery Standard..... | 8 |
| Account Transition Standard | 10 |

Social Media Application


All institutional social media accounts must be approved through a formalized application process before the accounts may go live.

To apply, account managers must answer the following questions and email answers to Kevin Saghy, Senior Director of Social Media, at saghy.2@osu.edu. CC: socialmedia@osu.edu and the unit social media lead. The team will respond within a week from submission.

****Note: Not all page requests will be approved. If your application is not approved, University Marketing and your unit social media lead will work with you to further develop the proposed strategy or incorporate your group's content into existing brand channels.***

1. Who is your unit social media lead?
2. What social media channel(s) are you applying for?
3. Why would you like to/did you create a page and what are you hoping to accomplish?
4. What will the name and handle of the page be?
5. Who is your target audience?
6. Could this content be shared on an existing brand social media channel? If not, please explain why.
7. Do you have a dedicated account manager(s)? Do they have basic social media experience? Please share the name of your account manager(s) and their past relevant experience.
8. Have all designated account managers read the Institutional Social Media Accounts policy and accompanying Institutional Social Media Accounts Protocols and Standards (ISMAPS)?
9. Can your account manager(s) spend 7-10 hours/week on content creation and publishing? Can they produce relevant content for your audience at the required frequency?
10. Can your account manager(s) monitor your social media account at least daily?
11. Social media platforms like Facebook require advertising in order to reach more than 2-5% of your page's followers with your content. Though not required, have you considered making funds available for social advertising?
12. What will your content consist of and how will you acquire and organize it?
13. How will you define success for this proposed social media account?
14. How do you plan to track and share performance?
15. The chart below represents a one-month social media editorial calendar. Please fill out the calendar with 12-15 social media posts of example content that you would publish on your page.

Month 1

| Day | Post Copy | Creative example/description |
|---------|------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Example | The Schott will soon be heating up by a few thousand degrees! 🎓🔥 |  |
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |
| 11 | | |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | | |
| 16 | | |
| 17 | | |
| 18 | | |
| 19 | | |
| 20 | | |
| 21 | | |

| | | |
|----|--|--|
| 22 | | |
| 23 | | |
| 24 | | |
| 25 | | |
| 26 | | |
| 27 | | |
| 28 | | |
| 29 | | |
| 30 | | |

Social Media Accounts – Minimum Requirements

Institutional social media accounts representing The Ohio State University are expected to maintain a minimum set of requirements to ensure a shared quality standard. The following items must be audited annually for unit accounts, as stated in the Institutional Social Media for Marketing and Communications Purposes policy, but it is recommended that they are reviewed monthly and remedied if not up-to-date. Account managers must audit their accounts and submit their audit results to their unit social media leads and University Marketing by July 15 each year.

1. Account creation

- New social media accounts should be created through the established application process that addresses the intended platform(s), strategy, target audience(s), page manager(s) and performance tracking.
- Accounts should not be created if the content could be published through existing platforms, or if they cannot maintain the minimum publishing expectations outlined below.
- Institutional social media accounts must adhere to Ohio State's Information Security Control Requirements, specifically for "shared account management." unless the platform functionality requires otherwise.

2. Branding

- Accounts must visually represent The Ohio State University through proper use of logos in profile images.
- Profile images/avatars should be created using the avatar template available at brand.osu.edu.
- Images used in the cover, header or profile should accurately represent the college or unit represented by the account.
- The account description/bio should not lead viewers to believe the entity operates as an organization or nonprofit outside of the University.
- The account name should include a variation of The Ohio State University, Ohio State or OSU.
- A consistent naming convention should be used across all associated accounts.

3. Content / Consistency

- Content must be posted in a consistent manner with no extended periods absent of publishing. At no point should a week go by without published posts on an account, and best practice on most platforms is to publish daily.
- A calendar of pre-planned content should be created to ensure consistent scheduling.
- Content should align with The Ohio State University brand guidelines.
- Do not violate copyright laws. Be sure you have permission to use images, videos, and audio before posting.

4. Logins and Passwords

- At least two full-time people from your practice area should have access to social media accounts.
- Personal email addresses should not be used for login information – only OSU.edu accounts as possible.
- Passwords and account recovery information should be changed on a quarterly schedule, and passwords should not be stored outside of university-protected servers.

5. Best Practices

- Accounts should be active, timely and responsive. The ongoing attention that social media requires should be considered in your planning.
- Institutional accounts should be checked daily to ensure managers see and report information posted about possible crimes, violence, or harassment as set forth in the policy.
- Use a university-recommended scheduling program to better manage posting and account access.
- When possible, compelling images or video should be utilized to strengthen content quality.
- Performance metrics should be monitored, analyzed and reported to optimize content delivery.
- Be professional and respectful. Each post and interaction is a representation of the university.

Primary Account Criteria and Management

Primary accounts are defined as those university social media accounts that are most visible because 1) they have a large follower base with at least one account totaling 30,000 followers and/or 2) an individual's leadership position within the university.

The university utilizes an enterprise publishing tool to reduce risk and manage security for primary accounts. At the time of adoption of these guidelines, up to 30 seats are available for these primary accounts, which has influenced the definition of primary accounts below. These primary accounts must be enrolled in the publishing tool (Hootsuite at the time of policy adoption) for risk management. However, publishing to each account through the tool is not mandated due to documented performance increases and expanded capabilities offered through native publishing on certain platforms.

The current primary organizational social media accounts at Ohio State include:

- Ohio State enterprise accounts
- Ohio State Emergency Management
- The Ohio State University Wexner Medical Center
- Ohio State Alumni Association main accounts
- Wexner Center for the Arts
- Ohio State Athletics
- Brutus
- Ohio State Football
- Ohio State Men's Basketball
- The Ohio State University Marching Band

The primary individual social media accounts at Ohio State include:

- The University President (Michael V. Drake)
- Executive Vice President and Provost (Bruce A. McPheron)
- Athletics Director (Gene Smith)

Those managing primary accounts will be provided additional tools to help reduce security risks and make account management more efficient.

For future state of these guidelines, the university is undergoing a request for proposal (RFP) to secure a publishing/analytics/security tool that can accommodate a larger volume of accounts representing the university in an official capacity. Additional accounts will be expected to utilize this tool for added security once available. These may include:

- The Ohio State University Police Division
- Student Life primary accounts
- Ohio State's Comprehensive Cancer Center – James Cancer Hospital primary accounts
- Colleges and Academic Units
- Regional Campus primary accounts
- Ohio State Buckeyes varsity athletic team accounts

Account Takeover Standard

These standards are for social media account takeovers, when temporary control of the account is given to an outside person (“temporary manager”) for publishing and audience interaction. These guidelines explain the proper takeover parameters and etiquette, and they ensure both the account manager and the temporary manager have a shared understanding of responsibilities.

The account owner should take the following elements into consideration when granting an account takeover:

- The temporary manager should have a tie to the Ohio State community (e.g., staff member, faculty, student, alumni) or be involved with a relevant event or experience.
- The temporary manager should have a social media presence deemed appropriate by the account manager.
- If the temporary manager is a student, they should be in good academic standing with the university.

The account manager must inform the temporary manager of the responsibilities for a takeover. The temporary manager must confirm in writing they have reviewed the Institutional Social Media policy and ISMAPS, and agrees to do the following:

- **Do not change any of the account settings.**
- **Do not add friends, follow accounts or send individual messages.** Post only to the account as agreed upon and seek approval before publishing.
- **Do not share password or account information.** This is a violation the university’s *Responsible Use of Computing and Networking Resources* policy.
- **Post responsibly.** Do not post while driving. No alcohol, drugs or paraphernalia of any kind.
- **Do not post profanity, sexual content, or derogatory gestures.**
- **Do not violate the terms and conditions of the social platform.**
- **Acquire consent before filming others:** If a post features another person, the temporary manager must have consent before recording.
- **Adhere to applicable laws and university rules and policies, including but not limited to, the University’s Code of Student Conduct.**

If activity does not adhere to this standard, the account manager may remove posts per Procedure III.D of the Institutional Social Media policy, in reference to Ongoing Management of Institutional Social Media Accounts.

The temporary manager should do the following:

- **Plan ahead:** Make a story board and/or a publishing calendar and seek approval before implementing. The temporary manager should discuss the topics he/she wants to cover with the account manager.
- **Introduce themselves:** Give brief personal details (e.g., major, year in school) and affiliation with Ohio State.
- **Promote account handles/codes:** Share and promote the takeover among his/her network of friends.
- **Geofilters and stickers:** Get approval before using features and functions (e.g., geofilters, stickers).
- **Variety:** Incorporate a variety of images and formats into the takeover.
- **No self-promotion:** Act as an ambassador of Ohio State to promote Ohio State-related content.

The following outline is available as a guide for account takeovers.

| Account Takeover Outline | | | | | | |
|-----------------------------------------------------------|--|--|--|--|--|--|
| Goal: | | | | | | |
| What is the main story you are trying to get across? | | | | | | |
| Who are you talking to? | | | | | | |
| Why do you want to share this content through a takeover? | | | | | | |
| How will you execute this takeover? | | | | | | |
| Time Frame: | | | | | | |
| Planning: Suggested Themes and Ideas | | | | | | |
| Draft of Text: | | | | | | |
| Post-story learnings: | | | | | | |
| Metrics: | | | | | | |

Account Recovery Standard

Standards for recovering a hacked social media account.

1. Document who has access

Accounts can be hacked. Please save a record of the name and login email/phone number of all individuals with access to each of your social media accounts, securely stored with double verification required. Be sure to include those who have access to a third party publishing tool (e.g., Hootsuite) as well.

2. Recovering a lost account

- 1) Attempt a password recovery once. Be cognizant of potentially freezing access through too many recovery attempts.
- 2) Submit appropriate support requests.
 - a. Facebook: <https://www.facebook.com/hacked>
 - b. Instagram:
 - i. If you still have access: <https://help.instagram.com/368191326593075/>
 - ii. If you cannot login (bottom): <https://help.instagram.com/368191326593075/>
 - c. Twitter:
 - i. If you can log in, reset password and review this document: <https://support.twitter.com/articles/31796#>
 - ii. If you cannot log in and can do a password reset, review this document: <https://support.twitter.com/articles/185703#>
 - iii. If you cannot log in and cannot do a password reset, submit a support request immediately: <https://support.twitter.com/forms>
 - d. LinkedIn:
 - i. If you still have access: <https://www.linkedin.com/help/linkedin/answer/56363?query=account%20hacked>
 - ii. If you cannot login: <https://www.linkedin.com/help/linkedin/ask/TS-RHA>
 - e. YouTube:
 - i. If you still have access: <https://myaccount.google.com/secureaccount?pli=1>
 - ii. If you cannot login: <https://accounts.google.com/signin/recovery>
 - f. Snapchat: <https://support.snapchat.com/en-US/a/hacked-howto>
- 3) Reach out to University Marketing's social media team to determine if there is a platform representative who can be leveraged for quicker action.

- 4) Contact Hootsuite (if applicable) for assistance and awareness and CC: University Marketing team.
 - a. Carley White: carley.white@hootsuite.com
- 5) Change passwords on all other accounts, including Hootsuite, if possible.
- 6) Stakeholder Rapid Outreach: notify the following staff (1) which account was compromised; (2) if Ohio State has access to the account; and (3) what content has been posted on the account.
 - a. University Marketing (Social Media):
 - i. Kevin Saghy: saghy.2@osu.edu
 - b. Communications (Crisis Response):
 - i. Lindsay Komlanc: Komlanc.2@osu.edu
 - ii. Deb Guinan: Guinan.4@osu.edu
 - iii. Lauren Kulik: kulik.10@osu.edu
 - iv. Gail Martineau: Martineau.18@osu.edu
- 7) Depending on the severity of the situation, University Marketing will notify the Social Media Community of Practice to encourage review of account security.

3. Re-starting account

- a. Archive and hide/delete any posts published without your authorization.
- b. Review administrative settings and managers of the affected account. Remove all suspicious or unnecessary users until the situation has been resolved.
- c. Review direct messaging for unauthorized use. Offer explanation to anyone who was contacted without authorization with pre-approved messaging (see 3.e. below).
- d. Review about descriptions, contact information, links, and all other information on account pages. Reverse any changes.
- e. Contact University Marketing for pre-approved “we’re back”/”apology” messaging and image.
- f. Post pre-approved messaging once approved by University Communications.

Account Transition Standard

These standards should be followed to transition ownership of accounts or in the event that an individual leaves the organization. The primary objective is to maintain security and integrity of accounts while maintaining access across all platforms for the remaining collaborators.

Minimum Access Standards

- A minimum of two (2) Ohio State employees must have access to each account. This will ensure that if an individual is terminated, resigns or is otherwise unable to support the ongoing social media needs, a secondary user can take over.
- Institutional social media accounts must adhere to Ohio State's Information Security Control Requirements, specifically for "shared account management," unless the platform functionality requires otherwise.

Termination/Resignation of Account Owner

- In the case of a termination or resignation of an account owner, a secondary user must immediately change password(s) to all associated accounts.
 - Passwords should be updated within the social platform (e.g., Twitter) and within the broader social media tools (e.g., Hootsuite).
 - For Facebook and LinkedIn, the user must be removed by the account admin.
- Share the new log-in information with other account users but do not share via email.
- If attached to a personal account, change the primary email address associated with the social media account to prevent log-in details from being altered further. As best practice, an organizational email address (e.g., socialmedia@osu.edu) should be used when possible.
- If the unit maintains an encrypted password document/spreadsheet, enter the new log-in information.
 - The password document/spreadsheet should be encrypted and the password to access the file should be updated.
- An email should be sent to important stakeholders, all account users, University Marketing's social media team, and your unit social media lead, to inform everyone the former employee no longer has access to the social channels.
 - The email should identify the new point of contact.
- As a general best practice, passwords should be proactively changed every 90 days as an extra precaution.

Onboarding New Hire or New Account Owner

- Following their onboarding and required institutional data training, the existing account owner may provide log-in and password information to the new hire.
- New hire must review the social media policy and standards.
- New hire must possess contact information for all other account users.

Transfer of Individual Accounts

- For the transfer of accounts representing individuals in leadership positions, please consult University Marketing and the Office of Legal Affairs.