Office of Marketing and Communications

Institutional Social Media Account Protocols and Standards

The Institutional Social Media Account Protocols and Standards (ISMAPS) support the implementation of the Institutional Social Media Accounts for Marketing and Communications Purposes University 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. This 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.

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 University Policy, but it is recommended that the information is reviewed monthly by account managers and social accounts should be remedied to meet the protocols and standards if not up to date. Account managers must audit their accounts and submit their audit results to their unit social media leads and the Office of Marketing and Communications every year.

Account creation

- New social media accounts should be created through the established institutional account application process that addresses the intended platform(s), strategy, target audience(s), page manager(s), content development and performance tracking.
- 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.
- 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" (page 122), unless the platform functionality requires otherwise.

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 with a university login at https://brand.osu.edu/brand-guidelines/templates-tools/social-media
- Images used in the cover, header or profile should accurately represent the college or unit represented by the account. The image library in the Digital Asset Management system provides a wide range of photos to keep cover and header images current: https://dam.osu.edu/
- 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 for handles and names across all associated accounts.

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.
- A calendar of pre-planned content should be created to ensure consistent scheduling.
- Photo, video and graphic design content should align with The Ohio State University brand visual guidelines: https://brand.osu.edu/brand-guidelines/visual
- Do not violate copyright laws. Be sure you have permission to use images, videos, and audio before posting.
- Content posted should be relevant and strategic to your unit, goals and audiences. Do not use an auto-posting software that automatically shares content not relevant to your unit (e.g., software that automatically tweets the weather).
- If using artificial intelligence like ChatGPT to assist with copywriting, copy must be reviewed and edited by a staff member before publishing.

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 or osumc.edu email accounts. As best practice, an organizational email address (e.g., socialmedia@osu.edu) should be used when possible.
- If an individual is leaving the university and their osu.edu email address is being used as the main login for an institutional social media account, the unit must change the main login email address for that account at least seven days prior to that individual's last day working at Ohio State to avoid being shut out of that account.
- Passwords and account recovery information should be changed on a quarterly schedule, and passwords should not be stored outside of university-protected servers.

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 tool to better manage posting, account access and community engagement. Refer to the Social Media Community of Practice page for more information on how to access these tools: https://omc.osu.edu/communities/social-media-community
- Ensure all social media content is accessible for all users. Refer to the Office of Marketing and Communications Social Media Accessibility Guide:

https://omc.osu.edu/social-media-community-practice/social-media-accessibility

- When possible, compelling images or video should be utilized to strengthen content quality.
- Images or video should be formatted to the ideal dimensions of the platform. Refer to these always up-to-date guides for social media image and video specs:
    - Social media image specs: https://sproutsocial.com/insights/social-media-image-sizes-guide/
    - Social media video specs: https://sproutsocial.com/insights/social-media-video-specs-guide/
- Performance metrics should be monitored, analyzed and reported to optimize content delivery.
- Be professional and respectful. Each post and interaction are 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 they meet at least one of the following criteria:

1) at least one account totaling 30,000+ followers
2) an account for an individual in a leadership position within the university
3) a college within the university

The university utilizes a third-party social media management tool to reduce risk and manage security for primary accounts. Primary accounts must be enrolled in the publishing tool with at least one active user for risk management; however, publishing to each account through the tool is encouraged but not mandated. There is a cost to be enrolled in the social media management tool and pricing has been set to make access possible for college and units of all sizes and budgets. To inquire about the cost and/or enrolling in the tool, reach out to: omc-scarletstudio@osu.edu.

Current primary organizational social media accounts at Ohio State include but are not limited to:

- 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
- The Ohio State University Marching Band
- Athletics teams that match the above criteria

Current primary individual social media accounts at Ohio State include but are not limited to:

- The University President

- Senior Vice President of Student Life
- President and CEO of the Alumni Association
- Athletics Director

Current primary college social media accounts at Ohio State include:

- College of Social Work
- College of Veterinary Medicine
- College of Arts & Sciences
- Fisher College of Business
- College of Dentistry
- College of Education and Human Ecology
- College of Engineering
- College of Food, Agriculture and Environmental Sciences
- John Glenn College of Public Affairs
- Moritz College of Law
- College of Medicine
- College of Nursing
- College of Optometry
- College of Public Health
- Graduate School
- College of Pharmacy
- Ohio State Online

Account Recovery Standard

Accounts can get hacked. These are the standards for recovering a hacked social media account.

Document who has access

Save a record of the name and login email/phone number of all individuals with access to each of your social media accounts. This information is required to be securely stored using multi-factor verification. Be sure to include those who have access to a third-party publishing tool (e.g., Sprout Social) as well.

Recovering a lost account

Attempt a password recovery once. Be cognizant of potentially freezing access due to too many recovery attempts.

Submit appropriate support request

- Facebook: https://www.facebook.com/hacked
- Instagram:
    - If you still have access: https://help.instagram.com/368191326593075/
    - If you cannot login (bottom): https://help.instagram.com/368191326593075/

- Twitter:
    - If you can log in, reset password and review this document: https://help.twitter.com/en/safety-and-security/twitter-account-compromised
    - If you cannot log in and can do a password reset, review this document: https://support.twitter.com/articles/185703#
    - If you cannot log in and cannot do a password reset, submit a support request immediately: https://support.twitter.com/forms
- LinkedIn:
    - If you still have access: https://www.linkedin.com/help/linkedin/answer/a1340402?query=account+
    - If you cannot login: https://www.linkedin.com/help/linkedin/ask/TS-RHA
- YouTube:
    - If you still have access: https://myaccount.google.com/secureaccount?pli=1
    - If you cannot login: https://accounts.google.com/signin/recovery
- Snapchat: https://support.snapchat.com/en-US/a/hacked-howto
- TikTok: https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked

Reach out to the Office of Marketing and Communication's social media team to determine if there is a platform representative or a third-party management tool representative who can be leveraged for quicker action.

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.

- Office of Marketing and Communications Social Media: socialmedia@osu.edu
- Office of Marketing and Communications (Crisis Response):
    - Lindsay Komlanc: komlanc.2@osu.edu
    - Lauren Kulik: kulik.10@osu.edu

Depending on the severity of the situation, the Office of Marketing and Communications will notify the Social Media Community of Practice to encourage review of account security.

Re-starting account

- Archive and hide/delete any posts published without your authorization.
- Review administrative settings and managers of the affected account. Remove all suspicious or unnecessary users until the situation has been resolved.
- Review direct messaging for unauthorized use. Offer an explanation to anyone who was contacted without authorization. Contact the Office of Marketing and Communications for consultation on a "we're back" / "apology" messaging.
- Review about descriptions, contact information, links, and all other information on

account pages. Reverse any changes.
- Post messaging once approved by the Office of Marketing and Communications.

Shutting down imposter accounts

If you come across an imposter profile of an institutional social media account, immediately report the account as an imposter/impersonation within the platform and notify the Office of Marketing and Communications at socialmedia@osu.edu with (1) the name, details and link to the imposter/impersonation account; (2) the name and link to the institutional social media account that is being impersonated.

In severe cases, the Office of Marketing and Communications social media team can leverage a third-party cyber security tool to assist with shutting down the imposter account.

In most cases, a clear parody account or an account with a disclaimer in the bio does not qualify as an imposter/impersonation account.

Account Transition Standard

These standards should be followed to transition ownership of accounts or when 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.

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 and must change the main account email.
- Passwords should be updated within the social platform.
- For Facebook and LinkedIn, the user must be removed by the account admin.
- In the case of a termination or resignation of an account owner, if their individual university email address is being used as the primary login for an institutional social media account, the unit must change the primary login email address for that account at least seven days prior to that individual's last day working at Ohio State to avoid being shut out of that account. As best practice, an organizational email address (e.g., socialmedia@osu.edu) should be used when possible.
- Share the new login 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 login details from being altered further.
- If an account is accessed via a personal account (e.g., how a Facebook page is accessed via a personal account), remove the individual's access from the account.
- If the unit maintains an encrypted password document/spreadsheet, enter the new login 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, the Office of Marketing and Communication'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 best practice, passwords should be proactively changed every 90 days as a 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.
- New hire must review brand guidelines and resources on: https://www.brand.osu.edu
- New hire must review information and resources on the Social Media Community of Practice website: https://omc.osu.edu/communities/social-media-community
- Reach out to the Office of Marketing and Communications social media team to add the new hire to the Social Media Community of Practice group.

Transfer of Individual Accounts

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

Document History
Issued: 2019
Edited: February 2022
Edited: April 2023