



GREATER NAPLES FIRE RESCUE DISTRICT
BOARD OF FIRE COMMISSIONERS
Action Item Worksheet

NEW BUSINESS

Agenda Item: III. C.
Subject: Social Media Policy Revision
Meeting Date: August 5, 2026
Prepared By: Michelle Ughi, HR Director

Background

Staff, in collaboration with the Union, District counsel, and Union counsel, reviewed and updated the District's Social Media Policy #604 to clarify employee rights, responsibilities, and the appeal process for denied content requests.

Funding Source/Financial Impact

Not Applicable

Recommendation

Staff recommends approval of the revised Social Media Policy as presented.

Potential Motion

I move to approve and adopt the revised Social Media Policy #604, effective immediately.

Attachment

Revised Social Media Policy #604
Redlined Social Media Policy #604

Legal Review

This AIW and its contents have been reviewed by legal counsel for sufficiency.

- ☒ Approved
☐ Not Approved
☐ Not Applicable

Comments (if any):

Reviewed by: Lara Donlon

Date: 7/27/2026

	GREATER NAPLES FIRE RESCUE DISTRICT POLICY	
	POLICY# 604 Social Media	
Section: All		Page(s): 7
Approved Date: January 14, 2026		Revised: August 5, 2026

Purpose:

The District recognizes that social media can be a valuable tool for communication and community engagement. However, social media also carries significant risks, including reputational harm, confidentiality breaches, and legal liability. As public employees, District personnel are subject to public scrutiny and must conduct themselves in a manner that upholds the integrity of the Greater Naples Fire Rescue District (“District”). This Policy establishes expectations for responsible social media use, protects the District from unnecessary risk, ensures compliance with applicable laws, and provides clear guidance for employees participating in social media on or off duty. In the event that there is or exists a conflict between this policy and federal or state law that protects District employees’ right to engage in protected concerted activity, the policy shall be applied consistently with those laws.

Definitions:

Social Media includes all digital platforms and online communication methods used to post, share, store, or distribute content. Examples include, but are not limited to:

- Social networking sites
- Video and photo sharing sites
- Blogs, personal websites, and online journals
- Messaging and chat platforms
- Online forums, comment threads, and livestreams
- “Story” features, bios, reels, feeds, or any content viewable by others

This Policy intentionally avoids naming specific applications to remain adaptable to evolving technologies.

Policy:

604.1 GENERAL POLICY

Employees may participate in social media for personal or professional use. However, they must recognize that content posted online can become public and may impact the District, regardless of privacy settings.

Employees are expected to use social media responsibly, professionally, and consistently with all District policies, applicable state or federal laws that protect employees’ right to engage in protected concerted activity, and public safety obligations, including Policy 601 Conduct and Behavior and SOG 101.10 Disciplinary Guidelines.

604.2 PATIENT, INCIDENT, AND CONFIDENTIALITY PROTECTIONS

604.2.1 Patient Privacy

Employees shall not post, transmit, record, share, or store any photographs, videos, audio recordings, or written content containing personally identifiable information (PII) regarding patient information or material protected under HIPAA or the Florida Information Protection Act (FIPA).

604.2.2 On-Scene Content

Employees shall not post or share any “on-scene” images or recordings of emergency calls, incidents, victims, patients, fire investigations, or District responses without express written approval from the Fire Chief, PIO or designee.

604.2.3 Confidential Information

Employees shall not disclose confidential, proprietary, investigative, or personnel-related information obtained through their employment.

604.3 USE OF DISTRICT IDENTIFIERS, LOGOS, AND IMAGERY

604.3.1 Prohibited Uses

Employees shall not use, display, post, or reference any District facilities, stations, apparatus, equipment, radios, uniforms, PPE, logos, patches, insignia, seals, graphics, or other identifying materials on personal or other social media without prior written approval from the Fire Chief, PIO or designee.

This includes, but is not limited to:

- Photos or videos taken at District property or fire stations
- Images of coworkers or supervisors
- Photos or videos of District vehicles, tools, or equipment
- Content that depicts employees in District-provided uniforms or PPE
- Any material that could reasonably be interpreted as associated with the District

604.3.2 Profile Identification

Employees shall avoid adding any reference to the Greater Naples Fire Rescue District, including written references to “Greater Naples Fire Rescue,” “GNFRD,” District logos or patches, photos or videos of District facilities, apparatus, equipment, or uniforms, or any content that could reasonably identify the District, to personal bios, profile names, “story” identifiers, or similar features. If an employee chooses to reference their employment, such content must be accurate, professional, align with District values, and reflect positively and professionally on the District.

604.3.3 Representation of the District

Employees shall not create, operate, or contribute to any account, page, or online presence that appears to speak for, represent, or portray the District without explicit written authorization from the Fire Chief.

604.4 EMPLOYEE RESPONSIBILITIES

604.4.1 Personal Accountability

Employees are solely responsible for the content they post, including any liability resulting from such posting. Online content can be copied, forwarded, altered, or archived indefinitely, even when deleted.

604.4.2 Spokesperson Restrictions

Unless an employee's job duties explicitly include social media communication:

- Employees must not present themselves as District spokespersons.
- Employees posting about District matters must include a disclaimer such as: "The views expressed are my own and do not reflect the views of the Greater Naples Fire Rescue District."
- Employees shall not post any content on the District's social media sites without explicit written authorization from the Fire Chief, PIO, or designee.
- The spokesperson designation is a dedicated assignment under management operational control.
- As such, speaking for the District on social media is a dedicated assignment under the District's operational control.
- Unless an employee is explicitly assigned this role by the District, the employee's social media activity must remain strictly personal and employees are to refrain from creating the impression that they are acting as an official digital voice for the District.

604.4.3 Accuracy and Integrity

Employees must be honest and accurate online. Knowingly false, misleading, or unverified statements about the District or its employees are prohibited.

604.4.4 Respectful Conduct

All online activity must comply with the District's anti-harassment, discrimination, workplace violence, professionalism, and conduct standards, including Policy 601 Conduct and Behavior and SOG 101.10 Disciplinary Guidelines.

604.5 PERSONAL USE OF SOCIAL MEDIA

604.5.1 On-Duty Restrictions

Employees may not use social media during work hours unless the activity is work-related and authorized by a supervisor.

604.5.2 Privacy Settings

Employees are encouraged to use privacy settings but must assume all content may become public.

604.5.3 Off-Duty Conduct

Off-duty social media conduct that adversely affects job performance, the work environment, coworker performance, public trust, or the District's legitimate business interests is prohibited.

604.5.4 Use of District Email

Employees shall not use District email addresses to create or register personal social media

accounts.

604.6 OFFICIAL DISTRICT SOCIAL MEDIA

604.6.1 Public Information Officer (PIO)

The District's Public Information Officer (PIO) manages and oversees all official social media platforms, content, and messaging. All District social media sites or pages must be approved by the Fire Chief and administered by the Public Information Office, unless otherwise directed.

604.6.2 Official Page Standards

Where possible, each social media page shall:

- Include an introductory statement identifying the purpose and scope of the District's presence
- Link to the District's official website
- Clearly indicate the page is maintained by the Greater Naples Fire Rescue District and include District contact information
- State that opinions expressed by visitors do not reflect the views of the District
- Indicate that comments may be monitored and that obscenities, off-topic comments, or personal attacks may be removed
- Indicate that all content posted or submitted for posting is subject to public disclosure

604.6.3 Content Approval (Official Use)

All official posts, images, videos, or digital media representing the District or that could reasonably be tied back to the District, must be reviewed and approved by the PIO or Fire Chief before posting. No content may be posted in connection with the District without written authorization.

604.6.3.1 Approval Process for Use of District Materials

Employees seeking approval to use District materials for social media, official or personal, must follow this process:

1. Submit a written request through the chain of command identifying:
 - Purpose of the content
 - Specific media or imagery involved
 - How and where the content will be shared
 - Whether District property, equipment, or uniforms are involved
2. Division leadership reviews and forwards the request to the PIO.
3. The PIO evaluates the request for accuracy, appropriateness, and compliance.
4. Final approval or denial is issued in writing by the Fire Chief, PIO or designee within seven (7) days after receipt of the information.
5. No filming, recording, posting, or sharing may occur until written authorization is received.
6. If approval is denied in whole or in part, the District shall provide the employee with a written explanation detailing the reasons for the denial.
7. The employee shall have seven (7) business days to appeal to the Fire Chief.
8. The appeal may submit the original content as-is or include edits that address the District's concerns, along with an explanation of how the post aligns with its intended purpose.
9. Management will review the appeal and issue a final and binding decision within seven (7) business days thereafter.

Unauthorized use of District imagery, branding, property, or identity is subject to discipline under SOG 101.10 Disciplinary Guidelines.

604.6.4 Compliance and Records Management

- A. All District social media content must adhere to applicable laws, regulations, and District policies, including information technology and records management requirements. This policy is intended to comply with all applicable laws and is narrowly tailored to protect the District's legitimate business interests and does not prohibit or interfere with employees' right to engage in protected concerted activity.
- B. Social media content is subject to public records laws, and applicable retention schedules apply.
- C. Content must be managed, stored, and retrievable in accordance with open records and e-discovery requirements.
- D. Employees must comply with all copyright, trademark and publication laws when creating and posting content on behalf of the District.

604.6.5 Reporting Issues

Employees must promptly notify the PIO of misinformation, negative comments, reputational concerns, or any potential social media issues involving the District.

Sharing District Content on Personal Accounts

Employees wishing to share District-related content including photos, videos, branding, apparatus, or uniforms, on personal social media accounts must obtain prior written approval from the PIO or Fire Chief.

Employees shall not represent that they speak on behalf of the District unless expressly authorized in writing.

604.6.7 Ownership of Social Media Platform Accounts and Content

All District-related accounts and content belong to the District, and not the employee. All login information including, but not limited to, usernames, passwords, and two-factor authentication details are similarly owned by the District and must be provided to the District and stored securely. Employees with authority from the Fire Chief to join platforms or create content on existing platforms shall not use personal credentials for District accounts or alter access details. Employees with such authority are required to promptly transition District social media accounts as directed by the Fire Chief upon separation from employment, any leave of absence, or upon request. Any social media presence established by an employee on behalf of the District are considered works created for, and owned by, the District.

604.7 FIRE CHIEF AUTHORITY

The Fire Chief retains final authority over all District-related social media communications and posts referencing the District and may modify or remove such content at any time.

604.8 MONITORING, REPORTING, AND ENFORCEMENT

604.8.6 Monitoring

The District may review publicly accessible social media content to ensure compliance. The District will not request or require login information or other access to private accounts.

604.8.7 Reporting Violations

Employees should report potential violations to Human Resources, a supervisor, or the Fire Chief's Office.

604.8.8 Disciplinary Action

Violations of this Policy may result in disciplinary action under, but not limited to, Policy 601 Conduct and Behavior, SOG 101.10 Disciplinary Guidelines, and any other District policies, SOGs, SOPs, or CBA, up to and including termination.

604.8.9 Non-Retaliation

Employees will not be retaliated against for reporting concerns, participating in investigations, or exercising legally protected rights.

EMPLOYEE SOCIAL MEDIA POLICY ACKNOWLEDGMENT FORM

I acknowledge that I have received, read, and understand the District's Social Media Policy (Policy No. 604). I understand that:

1. I am responsible for complying with this Policy at all times.
2. Violations may result in disciplinary action.
3. I may direct questions to Human Resources, the PIO, or the Fire Chief.
4. The Fire Chief retains final authority over District-related social media matters.

Print Name: _____

Signature: _____

Date: _____

	GREATER NAPLES FIRE RESCUE DISTRICT POLICY	
	POLICY# 604 Social Media	
Section: All		Page(s): 7
Approved Date: January 14, 2026		Revised:

Purpose:

The District recognizes that social media can be a valuable tool for communication and community engagement. However, social media also carries significant risks, including reputational harm, confidentiality breaches, and legal liability. As public employees, District personnel are subject to public scrutiny and must conduct themselves in a manner that upholds the integrity of the Greater Naples Fire Rescue District (“District”). This Policy establishes expectations for responsible social media use, protects the District from unnecessary risk, ensures compliance with applicable laws, and provides clear guidance for employees participating in social media on or off duty. In the event that there is or exists a conflict between this policy and federal or state law that protects District employees’ right to engage in protected concerted activity, the policy shall be applied consistently with those laws.

Definitions:

Social Media includes all digital platforms and online communication methods used to post, share, store, or distribute content. Examples include, but are not limited to:

- Social networking sites
- Video and photo sharing sites
- Blogs, personal websites, and online journals
- Messaging and chat platforms
- Online forums, comment threads, and livestreams
- “Story” features, bios, reels, feeds, or any content viewable by others

This Policy intentionally avoids naming specific applications to remain adaptable to evolving technologies.

Policy:

604.1 GENERAL POLICY

Employees may participate in social media for personal or professional use. However, they must recognize that content posted online can become public and may impact the District, regardless of privacy settings.

Employees are expected to use social media responsibly, professionally, and consistently with all District policies, applicable state or federal laws that protect employees’ right to engage in protected concerted activity, and public safety obligations, including Policy 601 Conduct and Behavior and SOG 101.10 Disciplinary Guidelines.

604.2 PATIENT, INCIDENT, AND CONFIDENTIALITY PROTECTIONS

604.2.1 Patient Privacy

Employees shall not post, transmit, record, share, or store any photographs, videos, audio recordings, or written content containing personally identifiable information (PII) regarding patient information or material protected under HIPAA or the Florida Information Protection Act (FIPA).

604.2.2 On-Scene Content

Employees shall not post or share any “on-scene” images or recordings of emergency calls, incidents, victims, patients, fire investigations, or District responses without express written approval from the Fire Chief, PIO or designee.

604.2.3 Confidential Information

Employees shall not disclose confidential, proprietary, investigative, or personnel-related information obtained through their employment.

604.3 USE OF DISTRICT IDENTIFIERS, LOGOS, AND IMAGERY

604.3.1 Prohibited Uses

Employees shall not use, display, post, or reference any District facilities, stations, apparatus, equipment, radios, uniforms, PPE, logos, patches, insignia, seals, graphics, or other identifying materials on personal or other social media without prior written approval from the Fire Chief, PIO or designee.

This includes, but is not limited to:

- Photos or videos taken at District property or fire stations
- Images of coworkers or supervisors
- Photos or videos of District vehicles, tools, or equipment
- Content that depicts employees in District-provided uniforms or PPE
- Any material that could reasonably be interpreted as associated with the District

604.3.2 Profile Identification

Employees shall avoid adding any reference to the Greater Naples Fire Rescue District, including written references to “Greater Naples Fire Rescue,” “GNFRD,” District logos or patches, photos or videos of District facilities, apparatus, equipment, or uniforms, or any content that could reasonably identify the District, to personal bios, profile names, “story” identifiers, or similar features. If an employee chooses to reference their employment, such content must be accurate, professional, align with District values, and reflect positively and professionally on the District.

604.3.3 Representation of the District

Employees shall not create, operate, or contribute to any account, page, or online presence that appears to speak for, represent, or portray the District without explicit written authorization from the Fire Chief.

604.4 EMPLOYEE RESPONSIBILITIES

604.4.1 Personal Accountability

Employees are solely responsible for the content they post, including any liability resulting from such posting. Online content can be copied, forwarded, altered, or archived indefinitely, even when deleted.

604.4.2 Spokesperson Restrictions

Unless an employee's job duties explicitly include social media communication:

- Employees must not present themselves as District spokespeople.
- Employees posting about District matters must include a disclaimer such as: "The views expressed are my own and do not reflect the views of the Greater Naples Fire Rescue District."
- Employees shall not post any content on the District's social media sites without explicit written authorization from the Fire Chief, PIO, or designee.
- The spokesperson designation is a dedicated assignment under management operational control.
- As such, speaking for the District on social media is a dedicated assignment under the District's operational control.
- Unless an employee is explicitly assigned this role by the District, the employee's social media activity must remain strictly personal and employees are to refrain from creating the impression that they are acting as an official digital voice for the District.

604.4.3 Accuracy and Integrity

Employees must be honest and accurate online. Knowingly false, misleading, or unverified statements about the District or its employees are prohibited.

604.4.4 Respectful Conduct

All online activity must comply with the District's anti-harassment, discrimination, workplace violence, professionalism, and conduct standards, including Policy 601 Conduct and Behavior and SOG 101.10 Disciplinary Guidelines.

604.5 PERSONAL USE OF SOCIAL MEDIA

604.5.1 On-Duty Restrictions

Employees may not use social media during work hours unless the activity is work-related and authorized by a supervisor.

604.5.2 Privacy Settings

Employees are encouraged to use privacy settings but must assume all content may become public.

604.5.3 Off-Duty Conduct

Off-duty social media conduct that adversely affects job performance, the work environment, coworker performance, public trust, or the District's legitimate business interests is prohibited.

604.5.4 Use of District Email

Employees shall not use District email addresses to create or register personal social media

accounts.

604.6 OFFICIAL DISTRICT SOCIAL MEDIA

604.6.1 Public Information Officer (PIO)

The District's Public Information Officer (PIO) manages and oversees all official social media platforms, content, and messaging. All District social media sites or pages must be approved by the Fire Chief and administered by the Public Information Office, unless otherwise directed.

604.6.2 Official Page Standards

Where possible, each social media page shall:

- Include an introductory statement identifying the purpose and scope of the District's presence
- Link to the District's official website
- Clearly indicate the page is maintained by the Greater Naples Fire Rescue District and include District contact information
- State that opinions expressed by visitors do not reflect the views of the District
- Indicate that comments may be monitored and that obscenities, off-topic comments, or personal attacks may be removed
- Indicate that all content posted or submitted for posting is subject to public disclosure

604.6.3 Content Approval (Official Use)

All official posts, images, videos, or digital media representing the District or that could reasonably be tied back to the District, must be reviewed and approved by the PIO or Fire Chief before posting. No content may be posted in connection with the District without written authorization.

604.6.3.1 Approval Process for Use of District Materials

Employees seeking approval to use District materials for social media, official or personal, must follow this process:

1. Submit a written request through the chain of command identifying:
 - Purpose of the content
 - Specific media or imagery involved
 - How and where the content will be shared
 - Whether District property, equipment, or uniforms are involved
2. Division leadership reviews and forwards the request to the PIO.
3. The PIO evaluates the request for accuracy, appropriateness, and compliance.
4. Final approval or denial is issued in writing by the Fire Chief, PIO or designee within seven (7) ~~FX~~ days after receipt of the information.
5. No filming, recording, posting, or sharing may occur until written authorization is received.
6. If approval is denied in whole or in part, the District shall provide the employee with a written explanation detailing the reasons for the denial.
- 67 The employee shall have seven (7) business days to appeal to the Fire Chief.
- 78 The appeal may submit the original content as-is or include edits that address the District's concerns, along with an explanation of how the post aligns with its intended purpose.
- 89 Management will review the appeal and issue a final and binding decision within seven (7) business days thereafter.

Unauthorized use of District imagery, branding, property, or identity is subject to discipline under SOG 101.10 Disciplinary Guidelines.

604.6.4 Compliance and Records Management

- A. All District social media content must adhere to applicable laws, regulations, and District policies, including information technology and records management requirements. This policy is intended to comply with all applicable laws and is narrowly tailored to protect the District's legitimate business interests and does not prohibit or interfere with employees' right to engage in protected concerted activity.
- B. Social media content is subject to public records laws, and applicable retention schedules apply.
- C. Content must be managed, stored, and retrievable in accordance with open records and e-discovery requirements.
- D. Employees must comply with all copyright, trademark and publication laws when creating and posting content on behalf of the District.

604.6.5 Reporting Issues

Employees must promptly notify the PIO of misinformation, negative comments, reputational concerns, or any potential social media issues involving the District.

Sharing District Content on Personal Accounts

Employees wishing to share District-related content including photos, videos, branding, apparatus, or uniforms, on personal social media accounts must obtain prior written approval from the PIO or Fire Chief.

Employees shall not represent that they speak on behalf of the District unless expressly authorized in writing.

604.6.7 Ownership of Social Media Platform Accounts and Content

All District-related accounts and content belong to the District, and not the employee. All login information including, but not limited to, usernames, passwords, and two-factor authentication details are similarly owned by the District and must be provided to the District and stored securely. Employees with authority from the Fire Chief to join platforms or create content on existing platforms shall not use personal credentials for District accounts or alter access details. Employees with such authority are required to promptly transition District social media accounts as directed by the Fire Chief upon separation from employment, any leave of absence, or upon request. Any social media presence established by an employee on behalf of the District are considered works created for, and owned by, the District.

604.7 FIRE CHIEF AUTHORITY

The Fire Chief retains final authority over all District-related social media communications and posts referencing the District and may modify or remove such content at any time.

604.8 MONITORING, REPORTING, AND ENFORCEMENT

604.8.6 Monitoring

The District may review publicly accessible social media content to ensure compliance. The District will not request or require login information or other access to private accounts.

604.8.7 Reporting Violations

Employees should report potential violations to Human Resources, a supervisor, or the Fire Chief's Office.

604.8.8 Disciplinary Action

Violations of this Policy may result in disciplinary action under, but not limited to, Policy 601 Conduct and Behavior, SOG 101.10 Disciplinary Guidelines, and any other District policies, SOGs, SOPs, or CBA, up to and including termination.

604.8.9 Non-Retaliation

Employees will not be retaliated against for reporting concerns, participating in investigations, or exercising legally protected rights.

EMPLOYEE SOCIAL MEDIA POLICY ACKNOWLEDGMENT FORM

I acknowledge that I have received, read, and understand the District's Social Media Policy (Policy No. 604). I understand that:

1. I am responsible for complying with this Policy at all times.
2. Violations may result in disciplinary action.
3. I may direct questions to Human Resources, the PIO, or the Fire Chief.
4. The Fire Chief retains final authority over District-related social media matters.

Print Name: _____

Signature: _____

Date: _____