MORROW COUNTY CLEAN WATER CONSORTIUM

RESOLUTION NO. 26-06

A RESOLUTION ADOPTING A SOCIAL MEDIA POLICY

WHEREAS, the Board of Directors ("Board") of the Morrow County Clean Water Consortium ("Consortium) desires to utilize social media platforms to communicate and engage with community members regarding the Consortium's activities; and

WHEREAS, the Board seeks to establish guidelines for the proper and efficient use of social media for this purpose;

NOW, THEREFORE, the Board hereby resolves as follows:

The Social Media Policy attached hereto as Attachment A is hereby adopted.

APPROVED this 8 th of September, 2026.

AYE VOTES: 3

NAY VOTES: Ø

ABSTAIN: Ø

ABSENT: 1

SIGNED:

David Sykes, Board Chair

ATTEST:

Board Secretary

ATTACHMENT A

MORROW COUNTY CLEAN WATER CONSORTIUM

SOCIAL MEDIA POLICY

The Morrow County Clean Water Consortium ("Consortium") wishes to use social media, such as Facebook, Instagram, LinkedIn, and Threads, to promote the interests of the Consortium while preventing and minimizing negative outcomes. This Social Media Policy establishes expectations and guidelines for the Consortium's use of social media.

DEFINITIONS. For purposes of this Policy:

1. "Social media" includes all means of communicating or posting information or content of any sort on the Internet, including to the Consortium's own or to a third party's web log or blog, journal or diary, personal or commercial website, social networking website, web bulletin board or a chat room, whether or not associated or affiliated with the Consortium, as well as any other form of electronic communication.

2. "Employee" shall include any employee of the Consortium; any contractor providing management services to the Consortium and subject to the direction of the Consortium's Board of Commissioners; or any person formally authorized to manage the Consortium's social media accounts, whether paid or unpaid by the Consortium.

OWNERSHIP.

1. Any content on the Consortium's official social media accounts will be considered property of the Consortium. The Consortium reserves the right to monitor such activity without prior notice to the individual posting the content.

2. The Consortium will have access to all information associated with its official accounts at all times, including access to usernames and passwords. The Consortium has the right to review, edit, and delete content associated with its accounts at any time.

3. If an employee separates from the Consortium, the Consortium has the right to assume control of any social media account owned by the Consortium and controlled by the employee.

4. No employee shall be asked to provide usernames, passwords, or any other information that would permit the Consortium to access their personal social media accounts. However, nothing in this Policy prohibits the Consortium from requiring an employee to produce content from his/her social media or internet account in connection with a Consortium-sponsored investigation into potential misconduct, unlawful or unethical behavior, or policy or rule violations.

CONTENT AND USE.

1. Social media sites may be used to conduct organizational business, as long as the use is authorized and complies with all applicable Consortium policies. Posts should avoid endorsing any business or product.

2. Consortium logos or other organizational information must conform to pre-approved marketing concepts and standards.

3. All posts on the Consortium's social media accounts, or posts made on other sites by a representative of the Consortium while acting in their official capacity, are public records which must be retained and disclosed as required by Oregon's Public Records Laws. Anyone posting information on a social media site while acting in their official capacity as a representative of the Consortium has no right to confidentiality with respect to such activity.

4. The Consortium reserves the right to establish rules of conduct applicable to third parties who post comments or responses on the Consortium's social media accounts, and to remove content that could reasonably be determined to be threatening, obscene, harassing, or abusive, or which contain images or links that may be harmful to Consortium systems or operations. The Consortium shall exercise care not to enforce rules arbitrarily or to remove third-party content solely on the basis of viewpoint.

EMPLOYEE CONDUCT.

1. Any employee using Consortium-provided computers or cell phones, or who is representing the Consortium through a social networking activity, is expected to represent the organization accurately and in a professional and positive light.

2. Employees are required to avoid engaging in harassing or unprofessional behavior when using or consuming social media, and to abide by all applicable laws and ethical considerations. Employees are expressly prohibited from posting content on any site that is malicious, abusive, threatening, intimidating, coercing, profane, disruptive, discriminatory, or harassing. Defamatory statements are prohibited. Employees may be personally responsible for the legal consequences of such statements.

3. Employees shall not use the Consortium's social media accounts for personal use.

4. Employees shall not conduct personal business on social media sites during work hours unless on an authorized work break, or when using Consortium-provided equipment.

5. No employee shall use official Consortium accounts to express personal opinions. When expressing a personal opinion or otherwise engaging in personal conduct that relates to or may affect Consortium operations, employees shall clearly explain that they are acting in their personal capacity and not on behalf of the Consortium, and that their views do not represent those of the Consortium, its employees, or its elected or appointed officials.

6. No employee may act as a spokesperson for the Consortium without formal authorization. When acting in their official capacity, employees shall identify themselves as representing the Consortium.
7. Any employee who fails to comply with this Policy may be subjected to discipline, up to and including termination.
8. Nothing in this Policy should be interpreted as limiting an employee's right to engage in legally protected speech or other activity, or to exercise any other rights available to the employee under state or federal law.

INTERNET HYGIENE.

1. Social networking sites may use phishing (e-mail messages asking for username and passwords, etc.) and spamming to collect profile information for marketing purposes or to engage in criminal activity. Viruses and spyware may damage the Consortium's operating system, compromise data, or expose the privacy of those operating or posting on social media sites.
2. As with any Internet use, never click on links asking for personal or confidential information, and heed security warnings and pop-ups. If possible, disable the ability of outside users to post HTML comments to the home page of any Consortium social media account. When in doubt about a link or message, delete it.
3. Be cautious making comments or posts that reveal personal travel plans or divulge other safety-sensitive and private information.