Social Media Best Practices for Wisconsin State Agencies

Introduction

Social media offers Wisconsin government the opportunity to engage with citizens and to facilitate transparency, interactivity, and collaboration. Using social media technologies is a business decision, not a technology-based decision.

The purpose of this document is to provide guidelines and highlights of best practices for social media use by state agencies. These guidelines and best practices may be used to develop agency-specific policies and procedures.

Best Practices

1) **Create an agency social media policy -** Each agency is encouraged to create an internal policy to govern how their social media accounts are created and managed. Social media platforms are available to a worldwide audience and you should take great care when using them. A social media policy, whether broad in terms or tool-specific, should include at a minimum:
    - Who has authority to create and agree to the social media tools, Terms of Service (TOS), etc.
    - What is acceptable content.
    - Who has the authority to create a social media account.
    - How access and security are managed.
    - How to handle records retention.

2) **Defining procedures to include these essential elements -** Once implemented, state agency social media sites should consider implementing procedures that include the following elements:
    - An introductory statement that specifies the purpose and scope of the social network site.
    - Links to the official state agency internet site for forms, documents, and other information.
    - Make sure appropriate options for capturing site content is in place if the content is 1) agency content not maintained in any other location or 2) posted by a member of the public.

3) **Make sure you review the social media platform policies**

    Privacy - State agencies should review the privacy policy of social media sites to determine if it is consistent with federal and state privacy obligations. In addition, review should be made of policy on data stewardship. Attention should be paid to the privacy policy to determine implications on end users, including but not limited to whether the policy:
    - Permits companies to track users of government websites for advertising purposes.
    - Allows access/disclosure of user information, including usage history.
    - Allows for selling user-provided information.
    - Allows for recording information about site usage.
    - Allows for opting out of any data collection processes.
    - States where the data will be physically maintained.

    If the agency uses persistent cookies on its own site, the agency should review that decision with its Public Information Officer (PIO) to assure that agency behavior is consistent with its privacy policy.

    Terms of Service (TOS) - Typically, a TOS is associated with the use of third-party social media tools. Each tool usually has its own unique TOS that regulates how users employ the tool. To avoid violations, any employee implementing social media on behalf of a state agency should consult the most current TOS and review it with the agency's PIO. If the TOS contradicts agency policy, the PIO should be made aware of it and a decision should be made about whether use of such media is appropriate.
    Wherever possible, state agencies, departments, and employees must consider at least the following:

- Who is authorized to open a "free" account with a third-party provider, which entails agreeing to TOS
- Who will read a TOS, prior to entering such agreements, to determine whether the TOS contains:
    - Terms that are problems for the agency or that are "deal breakers".
    - Terms that are a good fit for the intended purpose.
    - Provisions that require the agency to monitor use.
    - Benefits of the platform that outweigh the risks.
- Who will monitor provider's site for unilateral amendments to TOS
- Who will determine how amendments will be addressed

4) **Manage content legally -** It is critical that agencies comply with laws governing copyrights. Agencies must also respect individual privacy rights. When posting materials, agencies should:
    - Obtain copyright releases for all material protected, or indemnification from the entity for which the material is to be posted.
    - Obtain model releases for each image (including video) of a person who may have a potential claim to such a right, or indemnification from the entity for which the material is to be posted.
    - If the agency receives proper notification of possible copyright infringement, it will remove or disable access to the allegedly infringing material and terminate the accounts of repeat infringers.
    - Use of limited excerpts of a copyrighted work may fall within the "Fair Use" Doctrine which allows certain limited uses of such excerpts without constituting an infringement of copyright.

5) **Mitigate security risks -** Whether employees are using social media sites on behalf of the agency or their personal accounts, employees need to be aware of current and emerging threats that they may face using social media website and how to avoid falling prey and posing a risk to the state network. If agencies participate in social networking, agencies should:
    - Use a separate user IDs and password to access social networking sites.
    - Never duplicate user IDs and passwords across multiple social networking sites.
    - Train and educate users about what information to share, with whom they can share it, and what not to share.
    - Help employees set appropriate privacy settings for social networking websites.
    - Update current Acceptable Use Policies to cover user behavior for new media technologies.

6) **Records Retention -** In the State of Wisconsin, the determination to retain a record is based on the content of the record, not the media. An agency should address the requirements for evaluating and retaining each unique type of record which may be created on a social networking site. Agencies should follow the retention of Public Records based on Wis. Stats. 16.61. Within these statues are the guidelines for Public Records on Social Networking Sites. Public Records on Social Networking Sites

   General guidance - Information posted by agencies to social networking sites is likely to be a public record and must be retained according to the relevant General Records Schedule (GRS) or agency Records Disposition Authorizations (RDA) in situations where any of the following apply:
    - The information is unique and not available elsewhere.
    - Contains evidence of the agency's policies and procedures.
    - Is being used to conduct the agency's work.
    - Has been authorized by the agency, or contains information for which there is a business need.

   When citizens post information concerning any aspect of agencies' work to agencies' social networking sites, that information likely is a public record and must also be retained according to a GRS or RDA; or when citizens use information from agencies' web pages or other social networking sites to create their own compilations on the sites (lists, directories, chronologies, etc.), such repurposed information meets the definition of a public record only when it is available to all other citizens using the sites when deemed appropriate. If the compilations are private and available only to the citizens who created them, they are not public records.