public works, roads & transport
MPUMALANGA PROVINCE
REPUBLIC OF SOUTH AFRICA

SOCIAL MEDIA GUIDELINES SUMMARY

Table of Contents

1. The Context 2
2. Account Management 2
3. Acceptable Use 2
4. Content 2
5. Government Communication Policy 2
6. Security 2
7. Leagal Issues 2
8. Citizen Conduct 2
9. Monitoring 2

SOCIAL MEDIA GUIDELINES SUMMARY

1. THE CONTEXT

- Social media channels include blogs, podcasts, wikis, and social networks such as Facebook, Twitter, YouTube, Instagram, Tumblr, and LinkedIn.
- Two-way communication is possible between government and citizens.
- Social media presents new challenges in navigating the line between official and personal use.

2. ACCOUNT MANAGEMENT

- The Head of Communication (HoC) or their designate is responsible for developing a social media strategy and plan, overseeing the creation and management of social media accounts.
- Each department must appoint an employee to liaise with the HoC and manage social media accounts, maintain a list of official and active accounts, ensure compliance with branding guidelines and monitor content.

3. ACCEPTABLE USE

- Only authorised personnel can discuss government operations on official social media sites.
- Employees recognised as official representatives cannot provide commentary that is contrary to official government positions on social media.
- Government employees using social media in their private capacity must declare upfront that they are writing personally and must adhere to relevant laws and regulations.

4. CONTENT

- Social media content must adhere to Government Online Content Guidelines, be professional, and reflect government values.
- Government resources should not be used for posting inappropriate or unlawful material.
- Employees must not disclose information about Government's physical or information security practices or procedures.

5. GOVERNMENT COMMUNICATION POLICY

- All content should reflect government values and be professional on both personal and official social media sites.
- Copyright protected content cannot be published.
- Fundamental principles for government employees engaging in social media include considering societal needs, providing relevant and timely information, demonstrating understanding and empathy, and responding to information requests promptly.
- Each government entity is responsible for ensuring current and relevant content, removing derogatory comments, responding to engagement, supporting campaigns through other media channels, and managing their own social media accounts.

6. SECURITY

- Entities must change social media account passwords twice a year and remove users who are no longer part of the operational team.
- It is recommended to use passwords that comply with the organizational IT security policy.

7. LEAGAL ISSUES

- Entities must keep a record of all posted information and correspondence on social media, which can be achieved using third-party services.
- Information and advice provided online must be captured, retained, and filed according to the National Archives and Records Service policy.
- Removed content must be retained, including the time, date, and poster's identity.

8. CITIZEN CONDUCT

- Government entities must inform citizens of the social media policy when interacting with the government.
- Social media commentary by citizens will be removed if it defames, insults, abuses, harasses, threatens, attacks, contains offensive language, discriminates, promotes commercial interests, or engages in illegal or unethical activities.
- Repeat violators must be blocked, deleted, and reported to the service provider.

9. MONITORING

- Social media accounts should be monitored daily for adherence to guidelines, comments, inquiries, and negative online sentiments.