**Administrative Policy 5: Social Media**
**Review/Revision Index**
**Original Acceptance Date: June 16, 2016**

- Reviewed June 21, 2018
- Revision 1 – Accepted August 20, 2020
- Reviewed September 6, 2022
- Reviewed August 15, 2024

**WORKFORCE DEVELOPMENT BOARD, INC.**
**ADMINISTRATIVE POLICY 5**

**SUBJECT:**
Social Media

**PURPOSE:**
The purpose of this policy is to provide guidance to the Area 17 One-Stop Operator and WIOA service provider for professional use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, texting, social networking sites, and other sites and services that permit users to share information with others in a concurrent manner.

**PROCEDURE:**
The following principles apply to professional use of social media on behalf of matters and services related to the Workforce Development Board, Inc. (WDB), as well as personal use of social media when referencing WDB or WDB business.

1. Staff must know and adhere to the service provider's code of conduct, personnel policies, and any other relevant policies when using social media in reference to the WDB and Area 17.

2. Staff should be aware of the effect their actions may have on their image, as well as the WDB's image. The information posted or published will become public record, and as such may be prohibited by WDB policies or as set forth in this policy.

3. Staff should be aware that the WDB may observe content and information made available by staff through social media. Staff should use their best judgment in posting material that is neither inappropriate, nor harmful to the WDB, its stakeholders, or consumers.

4. Some specific examples of prohibited social media conduct include, but not limited to: posting commentary, content or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.

5. Staff are not to publish, post, or release any information that is considered confidential or not public. If there are questions about what is considered confidential, staff should consult with their supervisor.

6. Social media networks, blogs and other types of online content may generate press and media attention or legal questions. Staff should refer these inquiries to the Board Director or designee.

7. If staff encounter situations while using social media that threaten to become antagonistic, staff should disengage from the dialogue in a polite manner and seek the advice of a supervisor.

8. Staff must attain permission before referring to or posting images of current or former customers, staff, WDB members, vendors, or partners. Staff must also gain appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.

9. Social media use should not interfere with the staff's duties and responsibilities to the service provider or the WDB. When using WDB or service provider computer systems, use of social media for business purposes is allowed, but personal use of social media is discouraged.

10. Subject to applicable law, after-hours online activity that violates any relevant policy may subject staff to the service provider's disciplinary procedures.

11. If staff publish content after-hours that involves work or subjects associated with the WDB, a disclaimer must be used, such as: "The postings on this site are my own and may not represent the Workforce Development Board's positions, strategies or opinions."

12. Staff shall keep WDB-related social media accounts separate from personal accounts.

**ACTION REQUIRED:**
All service provider staff will refer to this policy when using social media to publish, post, or discuss Board activities or services.

If the service provider decides to establish professional social media accounts, the following elements can assist with developing an internal process.

<u>Employee Access</u>

a. Define which employees will officially represent your agency's interests through social networks.
b. Define authorization process for employees wanting to create an account.
c. Define employees' access for professional interests.
d. Define whether or not employees can access social networking sites for personal use during business hours.
e. Define when and how employees' personal use intersects with the agency's interest.
f. Define disciplinary actions based on legal precedent.

<u>Account Management</u>

a. Define who will set up the social media accounts.
b. Define procedure(s) for establishing an account.

c. Define who will track the social media accounts and how they will be tracked.
d. Define who will close social media accounts.

Acceptable Use and Employee Conduct

a. Define which acceptable use policies apply to social networking sites from already existing online communications policies.
b. Define what can and cannot be stated on social media platforms in an official capacity.
c. Define why and how employees should present themselves and your agency on social media platforms in an unofficial capacity.
d. Define how conduct reflects upon employees.
e. Define disciplinary actions if inappropriate usage occurs.

Acceptable Content

a. Define purpose and scope of presence on social media platforms.
b. Determine which office or individual will be the "gatekeeper" regarding what is acceptable and what is not.
c. Clearly state how communications will reflect upon your agency.
d. Define what can and cannot be shared.
e. Define when it is appropriate for employees to post an opinion.
f. Define disciplinary action if inappropriate content is posted.

Security

a. Define who will maintain usernames and passwords for social media accounts.
b. Provide information on what constitutes personally identifiable information.
c. Define and provide training on how employees can establish privacy settings on social media platforms.
d. Define who will be responsible for overall security to include developing and delivering training.
e. Define geo-tagging and appropriate usage.
f. Provide awareness and protections against phishing scams and viruses.
g. Describe and define what will happen if a security breach does occur.

Legal Issues

a. Define what and how public records laws and the Freedom of Information Act applies to usage.
b. Define who will be responsible for maintaining records.
c. Define and write disclaimers to be used on all content regarding laws that apply to usage.
d. Define how freedom of speech/First Amendment rights apply to content.
e. Define and address user accessibility rights.
f. Define Terms of Service or Terms and Conditions outlined by the third-party platforms.

Citizen Conduct

a. Outline expectations of citizen conduct.
b. Write and post comment policy, including when comments will be removed.
c. State what will happen with removed content (e.g. records retention).

**CLARIFICATION:**
Any clarification on the above policy should be directed to the Board Director.

**EFFECTIVE DATE:**
Immediately