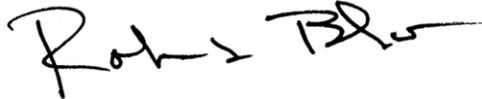


## REQUIREMENTS FOR LAUNCHING DAS SOCIAL MEDIA PLATFORMS

POLICY NUMBER: 10-01	EFFECTIVE DATE: July 31, 2012	APPOINTING AUTHORITY APPROVAL: 
AUTHORITY: Ohio IT Policy ITP-E.8, "Use of Internet, E-mail and Other IT Resources" (3/19/2008)		

### 1.0 PURPOSE

The purpose of this policy is to notify Department of Administrative Services (DAS) divisions/program areas of the requirements for launching a DAS social media platform. For the purposes of this policy, social media is defined as any technology platform designed for social interaction, using highly accessible and scalable publishing techniques. Examples of such tools are Facebook, YouTube, Twitter, LinkedIn, Google+ and SlideShare.

This policy outlines the application, justification, content management, privacy, security, terms of service, public records, accessibility and training requirements associated with operating a DAS social media platform.

### 2.0 SCOPE

This policy applies to all DAS divisions/program areas seeking to launch an official DAS social media presence. This policy is not meant to address the personal use of social media channels by DAS employees, contractors, temporary personnel and other agents of the state. Those requirements are addressed in Ohio IT Policy ITP-E.8, "Use of Internet, E-mail and Other IT Resources," and DAS Policy 700-01, "Information Technology Resource Usage."

### 3.0 BACKGROUND

Social media channels offer an opportunity for DAS divisions/program areas to communicate quickly and effectively with peers, customers, and the citizens of Ohio. A number of Ohio agencies are already taking advantage of the benefits of social media, as evidenced on the Ohio Social Media Web page, <http://www.ohio.gov/social/>. While DAS recognizes the value of social media, it is important to outline some general rules for engagement. It is essential that regardless of the communication channel that DAS maintain an official, professional presence.

This policy provides requirements that are meant to ensure that there is a deliberate, strategic process behind launching an official DAS social media presence. Due to the fact that there is a certain degree of risk associated with participating in this type of communication channel, it is important to clearly outline the requirements for all potential participants. Each application will be carefully reviewed by DAS Communications and DAS Legal to ensure that engagement in the

proposed social media channel is what makes sense for DAS and for Ohio. To receive approval for participation, all of the stipulated requirements must be satisfied.

## **4.0 REFERENCES**

- 4.1 DAS Policy 100-02, “Work Rules”
- 4.2 Ohio IT Policy ITP-E.8, “Use of Internet, E-mail and Other IT Resources”
- 4.3 DAS Policy 700-01, “Information Technology Resource Usage”
- 4.4 Ohio IT Policy ITP-E.30, “Electronic Records”

## **5.0 POLICY**

Prior to launching a social media presence in support of a DAS division/program area’s goals and objectives, a formal justification shall be provided to DAS Communications. DAS Communications shall work with DAS Legal to validate that overall management, content, security, privacy, terms of service, public records, accessibility and training considerations are sufficiently addressed in the division/program area’s proposal. A “Request for Launching a DAS Social Media Platform,” form shall be completed by the division/program/area and submitted to DAS Communications. The form is attached to this policy and the instructions for submission are detailed in section 6.0 Procedures.

The following policy sections outline the requirements that will be considered by DAS Communications and DAS Legal as part of the formal social media business justification review.

### **5.1 Social Media Strategy**

Social media presents a multitude of possibilities for DAS in terms of communicating with both internal and external customers. However, as with any communication channel, there are instances in which the use of a social media platform is more appropriate. As part of the justification, the DAS division/program area shall demonstrate that as a minimum, it has considered the following:

- Where social media fits within the current construct of the program’s current marketing strategy with clear consideration of the requirements, scope, audience and engagement level necessary.
- An adoption plan that takes into consideration the cost, resources, policy restrictions and current DAS division/program channels that will be created and diminished through the creation of the new channel.
- Are there existing communities in which the division/program area could participate and realize the same results? What existing conversations may be taking place where a DAS division or program area could add value? *This option would significantly lessen the degree of resource commitment involved with maintaining a social media presence.*

- Are there any other agencies, or DAS divisions/program areas that have already established a social media presence? Would it make sense to utilize any of the existing Ohio channels?
- Does research into other government entities, organizations, and businesses indicate that this path may also work for the DAS division/program area?
- What is the target audience and how does launching the proposed social media platform address their needs?
- Is there an exit strategy? Will the presence be maintained indefinitely? How will the division/program area determine if/when they should exit the use of a particular social media platform?

## **5.2 Content Management Considerations**

The appeal of social media is that it is very accessible, engaging, and interactive. While this is a benefit, it also represents a challenge for participating entities. Content must be dynamic and relevant; therefore, a more significant resource footprint is necessary to maintain content on a social media platform as opposed to a static Web page. To ensure that DAS divisions/program areas meet these demands, the following content management requirements shall be satisfied:

5.2.1 Content Management Process. DAS divisions/program areas shall develop and implement a well-defined content management process for releasing and retiring content.

- 5.2.1.1 The process shall include an approach to monitoring and replying to comments, if comments are enabled.
- 5.2.1.2 The expected level of interactivity on the platform shall also be clearly defined and communicated.
- 5.2.1.3 DAS divisions/program areas shall ensure that the necessary resources are assigned to keep content up to date. This includes the appointment of experienced, responsible content managers. As a minimum, two content managers shall be appointed to maintain the content.
- 5.2.1.4 All content management responsibilities must fall within allowable job duties. If a DAS division/program area needs guidance regarding the permissible use of resources for updating social media content both within and outside of normal working hours, they shall work with DAS Communications and the DAS Office of Employee Services to ensure that bargaining unit contracts are not breached.
- 5.2.1.5 DAS divisions/program areas shall clearly communicate to content managers the parameters for acceptable content. As a minimum, content managers shall understand that the following types of content are not acceptable:
  - Vulgar or offensive language

## *Requirements for Launching DAS Social Media Platforms 10-01*

- Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or developmental disability or sexual orientation
- Spam
- Content that advocates illegal activity
- Promotion of particular services, products
- Content that supports or opposes political campaigns or ballot measures
- Infringement upon copyrights or trademarks
- Information that may compromise the safety or security of the public or public systems
- Personal communications that are unrelated to official DAS business

5.2.1.6 DAS divisions/program areas shall outline a transition process for when, for whatever reason, a resource will no longer be serving as a content manager.

5.2.2 Account Creation. Only State of Ohio e-mail accounts shall be used to establish a social media platform. Under no circumstances shall an employee's personal email address be used to establish an official DAS social media presence. Further, DAS divisions/program areas shall use a common e-mail account to create and manage the social media presence. This approach prevents the social media account from being tied to a specific state employee.

5.2.3 Branding. In recognition of the importance of having a consistent look and feel across all DAS social media platforms, all DAS divisions/program areas shall work with DAS Communications on the platform design. A social media platform shall not be launched without receiving approval from DAS Communications. As a minimum, any DAS-branded social media platform shall contain the following common elements:

5.2.3.1 An Ohio.gov approved logo

5.2.3.2 A DAS approved logo

5.2.3.3 A link to the DAS home page

5.2.3.4 A link to Ohio.gov

5.2.4 Implied Endorsements. While a number of social media platforms sustain their existence by selling advertising space, as a government entity, the preference is that DAS content does not co-exist next to commercial advertisements. This is especially true when context sensitive advertisements, or advertisements that trigger based upon key words, are employed by the platform. This type of advertising could result in the appearance of advertisements that are contrary to the positions of DAS or the state as a whole.

DAS divisions/program areas shall work with DAS Communications to review platform settings, and when possible, elect to disable advertisements. If it is not possible to disable them, the DAS division/program area shall consider the use of disclaimers on the platform and any relevant Web pages. In addition, DAS divisions/program areas shall regularly monitor the platforms to ensure that the posted advertisements are appropriate.

## 5.3 Privacy Considerations

The interactive and casual format of social media can be a very promising way to engage citizens and customers, but it can also present a substantial risk to privacy. DAS divisions/program areas shall ensure that they have addressed privacy considerations as part of their social media platform planning process. This section addresses the elements that need to be addressed prior to launching a site in order to sufficiently mitigate the risk to privacy.

- 5.3.1 Protect Sensitive and Personally Identifiable Information. It is important that DAS divisions/program areas take the same care to protect sensitive<sup>1</sup> and/or personally identifiable information<sup>2</sup> on social media platforms as they do on other communication channels. DAS divisions/program areas shall ensure that content managers understand the difference between public content and sensitive and/or personally identifiable information. Failure to protect such information exposes not only DAS, but individual state employees to legal liability and could have a significant negative impact on Ohio’s citizens.
- 5.3.2 Conduct Privacy Impact Assessments. DAS divisions/program areas shall conduct a privacy impact assessment for any proposed social media platform. “Ohio Privacy Impact Statements and Assessments 2012,” outlines a process for conducting privacy impact assessments and privacy threshold analysis. Use of this tool will help ensure that personally identifiable information is handled in accordance with applicable legal, regulatory, and policy requirements. It will also help to determine the risks and effects of collecting, maintaining and disseminating information and evaluate alternatives for handling information that may assist in mitigating potential privacy risks.
- 5.3.3 Provide Privacy Policy Disclaimer. DAS divisions/program areas are also encouraged to include a disclaimer that advises users that they are no longer on a State of Ohio site and that the privacy policy of the social media platform applies. A link to the platform’s privacy policy shall also be included.

---

<sup>1</sup> “Sensitive data” is any type of data that presents a high or medium degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a medium risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. The data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

<sup>2</sup> “Personally identifiable information” is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

## **5.4 Security Considerations**

After approval but prior to launching a social media platform, DAS divisions/program areas shall ensure that all involved parties are aware of the potential security risks. Content managers as well as anyone responsible for maintaining the platform shall understand the following security implications:

5.4.1 Individual Security Risks. All social media platforms collect some type of personal profile information, including name, gender, location, employer, photographs, and names of friends, personal interests, and affiliations. If someone is able to gain access to this information, it could enable identity fraud and personal attacks. It could also result in the posting of fraudulent profile pages and messages, defamation, and theft of artwork or intellectual property.

5.4.2 Organizational Security Risks. Since organizational profile pages are only protected with a user ID and password, the organizational profile page can also become an object for attack. Organizations can also be subject to defamation and identity fraud, which can lead to damage to organizational image and reputation.

5.4.3 IT Infrastructure Risks. Social media platforms provide an opportunity to spread malicious code, such as viruses and worms. The ability to use mobile devices that allow the exchange of rich-media content, as well as text messages to engage in social networks, intensifies this issue.

5.4.4 Security Incident Response. DAS divisions/program areas shall ensure that a clearly defined incident response process is in place. If a content manager reports a suspected incident, the DAS Office of Information Security shall be immediately notified.

5.4.5 Standard Security Practices. Aside for the security protections that DAS OIT will employ to protect the platform, content managers shall understand that there are certain behaviors that they can engage in that will assist in improving security. Content managers shall:

- Use strong passwords (A combination of letters, numbers and characters)
- Safeguard passwords
- Change passwords regularly
- Only manage platform content with DAS approved/supplied applications (This requirement applies to mobile devices as well.)
- Monitor content on a regular basis to detect any unauthorized alterations
- Report any suspected security incidents to DAS division/program management as soon as possible

## **5.5 Terms of Service Considerations**

Each social media platform has its own unique terms of service. Some social media platforms offer terms of service that are tailored to governmental entities. Prior to agreeing to any specified terms of service, DAS divisions/program areas shall work with DAS Communications to determine the options available to governmental entities. Further, terms of service must be

discussed with DAS Legal Services before adoption to ensure that the division is legally able to agree to the provider's terms. If available, government terms of service shall always be adopted as opposed to standard terms and conditions.

## **5.6 Public Records Considerations**

DAS divisions/program areas shall be aware that any content posted on social media platforms could potentially be considered a public record; and therefore, must be retained in accordance with the appropriate DAS record retention schedules. Archival requirements shall also be considered when designing and updating social media platforms. It may be necessary to preserve versions of the platforms for a certain period of time.

If necessary, DAS divisions/program areas shall work with DAS Records Management to obtain clarification on retention requirements. Ohio IT Policy ITP-E.30, "Electronic Records," also outlines electronic record management requirements.

## **5.7 Accessibility Considerations**

As with all public-facing Web pages, DAS must strive to ensure that any content provided on social media platforms is accessible to all constituents. However, on third party social media platforms, it may not be possible to make all content accessible. There are third party social media platforms that do not provide access to transcripts or captioning, and for DAS divisions/program areas to include this functionality on their own would be extremely costly. Therefore, third party social media platforms shall not be the sole location where original content is posted. This will help ensure that all constituents have an accessible version of the content and that the official version is available on the DAS website. It is important to keep in mind that not all Ohio citizens utilize social media platforms.

## **5.8 Training Considerations**

It is expected that any DAS division/program area participating in social media shall take adequate steps to train content managers in all of the areas discussed within this policy. Specifically, the training shall include the requirements and considerations related to:

- Social media strategy
- Content management
- Privacy
- Security
- Terms of Service
- Public Records
- Accessibility

Content managers shall sign a statement indicating that they have received training and understand the responsibilities associated with content management on DAS social media platforms.

## **6.0 PROCEDURES**

- 6.1 The DAS division/program area interested in establishing an official DAS social media presence shall complete the attached form entitled, "Request for Launching a DAS Social Media Platform."
- 6.2 The completed form shall be sent to the appropriate DAS division deputy director for approval.
- 6.3 If approved, the form shall be forwarded to DAS Communications and DAS Legal for approval.
- 6.4 DAS Communications and DAS Legal will review the application and either request additional information, approve or deny the application.
- 6.5 If the application is approved, the DAS division/program area shall work with DAS Communications to develop an approved design for the platform.
- 6.6 Once the design is approved, the DAS division/program area may launch the social media platform and operate it as outlined within their application.
- 6.7 DAS Communications shall ensure that a link to the social media channel appears on the Ohio Social Media Web page, <http://www.ohio.gov/social/>.
- 6.8 DAS Communications shall periodically monitor all approved DAS social media channels.
- 6.9 Two years after approval and successful deployment, DAS Communications and the requesting DAS division/program shall perform a review of the channel to determine future direction.
- 6.10 DAS Communications or DAS Legal may at any time require that participation in a social media platform be disabled if they feel that the DAS division/program area is not adhering to the requirements of this policy, the original strategy outlined in the approved application, or if they feel overall management of the channel is not sufficient or appropriate.

## **7.0 INQUIRIES**

Direct inquiries about this policy to:

DAS Office of Communications and External Relations

Ohio Department of Administrative Services

30 E. Broad St., 40<sup>th</sup> Floor

Columbus, Ohio 43215

Email: [DASCommunications@das.state.oh.us](mailto:DASCommunications@das.state.oh.us); Subject: Social Media Platform Request

Telephone: 614.644.0194

## **8.0 REVISION HISTORY**

<b>Date</b>	<b>Description</b>
07/31/2012	Original policy

## **9.0 ATTACHMENTS**

**Form:** [Request for Launching a DAS Social Media Platform](#)