

Guidelines for Conducting Citizen Engagement, Specific to Social Media

Overview

In this document you'll find:

- A. The BC Public Service Philosophy and the Context for Change: Information about the context for and benefits of using social media tools.
- B. Key Considerations: The things to be aware of and a bit about the process to follow in using social media for public discussion.
- C. Principles: To guide the use of social media tools in your professional capacity.
- D. Summary and Further Information

A. The BC Public Service Philosophy and the Context for Change

Every day BC Public Service employees deal directly with the public, with stakeholder groups and with colleagues. They do that work professionally and responsibly, reflecting the trust placed in them by their employer and citizens. Social media is quickly becoming part of the everyday work of the public service and, in fact, many organizations.

Citizens increasingly expect greater responsiveness and input into decisions that affect them. They expect better access to services and more choice about how, when and where they get that access. Social media tools are not just tools for communication. They are tools for business, and can help us in our work with citizens and stakeholders.

Eventually, social media tools will just be part of the normal working experience for government employees, just like telephones and email. But, recognizing that social media tools are also new and unique in many ways, these guidelines have been developed to support the adoption and adaptation of these tools in the public service. They reflect some of the unique circumstances that apply to the public service, including the reality that citizens tend to expect greater accountability from government than most organizations. But overall these guidelines are based on one important philosophy: *we trust our employees to be responsible in their use of these tools, just as we trust them in every other aspect of their work.*

With these guidelines and the right training and support in place, we trust that employees will use these tools responsibly.

B. Key Considerations

Planning for the use of public social media tools (e.g. Twitter, Facebook) should include developing a business plan with intended outcomes, appropriate tools and resources required to support the project. As part of the planning process, the ministry or program area should have gone through a process that determines that social media tools are the best approach or one of a variety of approaches to engage the public.

Approvals: Social media tools are part of the tool set for engaging the public; therefore it is important no matter which tool, you make an assessment of potential communications issues for government. That might mean involving your supervisor, your executive, your deputy minister or even your Minister's Office in the approval processes, depending on the situation. You should involve your ministry's Public Affairs Bureau team if you think your project may create an issue for government. The training and information that supports these guidelines will provide examples of when to involve different areas in your approval process. But in general, you should evaluate the

Guidelines for Conducting Citizen Engagement, Specific to Social Media

use of social media tools and the required approvals the same way you would evaluate the risks and benefits of any other more traditional form of public engagement, keeping in mind that social media tends to be a more publicly visible approach to engagement.

Support: The Citizen Engagement team at the Ministry of Citizens' Services is available to support ministries with planning for the use of social media tools. Information specific to the range of tools that can be used for public engagement will be posted on @Work over time.

Managing Professional and Personal Use of Social Media

BC Public Service employees who comment on public social media sites in their professional capacity, or who wish to comment on work-related issues in their personal capacity, must adhere to the BC Public Service Standards of Conduct. Comments on social media sites on matters unrelated to work are employees' own concern.

Important sections of the [Standards of Conduct](#) to note are those respecting:

- *Loyalty:* Employees' conduct should instil confidence and trust, and must not bring the public service into disrepute.
- *Confidentiality:* Confidential information that employees receive through their employment must not be divulged to anyone other than persons who are authorized to receive the information.
- *Public comments:* Employees may comment on public issues, but must not engage in any activity or speak publicly where this could be perceived as an official act or representation (unless authorized to do so). Employees must not jeopardize the perception of impartiality through making public comments or entering into public debate regarding ministry policies, or use their position in government to lend weight to the public expression of their personal opinions.
- *Political activity:* If engaging in political activities, employees must not do so during work hours or using work equipment, and must be able to retain the perception of impartiality in relation to their duties and responsibilities.

If in doubt, employees may discuss the matter with their supervisor, and/or consider adding a disclaimer to their web presence, such as "these views are mine alone and do not represent those of the Government of British Columbia or the BC Public Service."

Planning for the use of social media must also include considerations for privacy, intellectual property, records management and information security. See more details on these in Appendix A.

C. Principles for Employees Participating in Social Media

Participating in social media means contributing content or comment. When doing so, we trust you to be professional, personable, and relevant.

Being Professional

When using social media sites in a professional capacity, you should identify your role as a BC Public Service employee. When in conversation, be a good judge of content. Keep in mind there are three important categories of information that cannot be discussed with members of the public in any forum - face-to-face or online: 1) matters before the courts; 2) draft legislation; and 3)

Guidelines for Conducting Citizen Engagement, Specific to Social Media

material about third parties (i.e., information about identifiable individuals) unless you have statutory authorization to do so.

Beyond these rules, two good tests for judging content include:

- “Does this content have a direct connection to my paid role?”—in an online discussion, only comment on topics on which you have responsibility and direct knowledge. Do not comment on areas outside your areas of responsibility. Refer out-of-scope questions to those with responsibility for those areas, or to the relevant communications officer.
- “Is this content something I would be comfortable saying in a public setting, such as a conference or stakeholder meeting?”—that is to say, be aware that your comments may be shared widely. Be sure to express your words and ideas in ways that do not undermine the reputation of yourself, your ministry or the BC Public Service.

Being Personable

Success in social media means not necessarily being formal in your online interactions. Being personable will help you build productive relationships, manage your own and your ministry’s reputation, and help you become a valued and proactive contributor to online conversations and communities. Draw on your experience to tell stories and anecdotes that illuminate your ideas, and use an authentic voice to help people connect to the person behind the title. In doing so, be mindful of the privacy guidelines in Appendix A - sharing too much may lead to compromises of your own or others’ privacy.

Being Relevant

Provide information that is timely and useful for your audience. Work hard to create conversations that are productive, and be responsive to questions and input that come in through your site. Consider inviting a colleague’s input before making a public posting. Talk to your PAB team if you want advice about how to create relevant content, and be sure to notify them if you receive a media request, including ones from bloggers who might be working on a story.

D. Summary and Further Information

These guidelines should underscore two key points. One, all BC Public Service employees are trusted to be responsible professionals in the use of social media. The second point is that we will strive to support employees in using social media, through information, training and discussion. Additional information will be accessible through @Work - that information will help employees and ministries consider and plan for appropriate use. That information will also further address how to manage risks and issues associated with using these tools.

This is the first iteration of these guidelines and they will continue to evolve over time as employees provide input and ask questions and we collectively gain more experience. If you have any questions at all about the use of social media in the workplace please email them to citizenengagement@gov.bc.ca. We will help where we can or forward your request to the appropriate subject matter expert.

Guidelines for Conducting Citizen Engagement, Specific to Social Media

Appendix A

Planning for the use of social media tools needs to include the following considerations:

Privacy

One of the biggest considerations in using social media is the protection of any personal information that is collected and disclosed. There are legislated restrictions through [The Freedom of Information and Protection of Privacy Act \(FOIPPA\)](#) to what government may collect, use and disclose. Personal information has a special meaning in FOIPPA, which is "information about an identifiable individual other than contact information" (with contact information meaning workplace address, telephone number or email etc. when used to contact that person at a place of business for a business purpose). The definition of personal information has a broad scope and includes, among other things, an individual's home address or email, appearance and image, educational and employment history, and personal opinions.

Because much of the content of social media sites contains personal information (i.e., user accounts containing personal profiles and pictures, comments containing opinions, images of people in photos or videos, etc.), FOIPPA plays a significant role in government's ability to use social media tools.

One of the first questions is to ask is if there is any personal information contained in the content - either content collected from a social media site, or content that is to be posted, i.e.:

- Does the content contain photos or videos containing identifiable individuals?
- Is the content about a particular individual?
- Is an individual expressing an opinion?

If there is no personal information FOIPPA does not apply, as there are no restrictions to posting text, video, photographs or other information that does *not* contain personal information (though there may be intellectual property, copyright, or confidentiality restrictions, as discussed below). For example: A comment without personal information might include a statement of fact or a website URL that does not point to an individual; a photo or video without personal information might be of a place or thing without an identifiable person in frame.

If, however, if you are planning to host or establish a social media tool as part of your ministry work (setting up a Twitter account, starting a Facebook group, YouTube channel, etc.), or if you are participating on behalf of your ministry (e.g. commenting on someone else's stream/feed in a way that collects, uses or discloses personal information) you should complete a [Privacy Impact Assessment](#) (PIA). The PIA will help you make sure your social media use is in keeping with FOIPPA.

'Collection' and 'disclosure' using social media are complicated. The Citizen Engagement team at the Ministry of Citizens' Services is available to support ministries and bring appropriate expertise in on this topic. Here are some of the details:

Guidelines for Conducting Citizen Engagement, Specific to Social Media

Collection

Personal information can be collected in a number of ways on a social media site. If planned content will contain personal information, *before collecting it* government must:

- Meet one of the requirements of the collection provision under FOIPPA. Consultation, service provision and communication purposes are laudable goals, but government must be able to demonstrate the collection relates directly to and is *necessary* for a program or the activity it is undertaking. Necessity is a strict test – it does not mean “it’s convenient” or “would be nice to have.” Much of the chatter of social media sites will not pass the “necessity” test.
 - Employees should consider stripping content of personal information before saving it, such as only saving peoples’ comments, not the names of the people who made them.
 - When using a government site to engage the public, you should also carefully consider how you pose questions as you do not want to elicit from the public more information than is “necessary”.
- Provide notice that ministries are collecting the information. This notice must include the specific authority under FOIPPA or other legislation for collecting the personal information, the purpose of the collection, and the contact information of an employee with the relevant program who can answer questions about the collection. Your design and use of a social media site must be planned so that this notice is given to anyone commenting or sharing information on the site.

Government may *not* collect personal information about a third party. For example: John Smith posts, “My wife, Jane Smith, needs to take daily doses of Medication A.” This post contains Jane’s personal information. In most cases, FOIPPA requires the collection of personal information be directly from the person it is about, and therefore you should not collect this information in personalized form. Posting information of this kind should be actively discouraged wherever possible through site moderation, explicit terms of use, and careful consideration of what types of questions to the public are posted to the site.

Ministries may wish to provide other channels for interaction, such as a government email address, for users who do NOT wish to share information with the Government of B.C. on social media sites.

Disclosure

Before *disclosing* personal information by posting it to a social media site, ministries should know that posting content to the Internet is a disclosure of personal information outside of Canada which requires special authority under FOIPPA.

Should government post content that contains personal information on a social media site (subject to intellectual property, copyright, and confidentiality, restrictions, as discussed below), the first question to ask is, “Who posted the personal information?”

- Government may re-post personal information that was originally contributed to a social media site *by the person it is about* and if the personal information was both compiled and is being disclosed for the purposes of public discussion and promotion of proposed or existing initiatives, policies, proposals, programs and legislation of your ministry. For example, if Jane Smith posts her opinion about a new piece of legislation on a government site or social media site, you may re-post her name and opinion.

Guidelines for Conducting Citizen Engagement, Specific to Social Media

- Government may not freely re-post personal information from other information sources, such as another website, photos, a newspaper article, government press release or ministry file. To do so, ministries must either have the written consent from the individual whose information is being disclosed or there must be legislation directing that the disclosure may take place. However, posting URLs and web addresses pointing to this information is permissible. You may want to investigate online consent as it relates to your project, as there are nuances under FOIPPA.

Intellectual Property

Intellectual property commonly used within government includes trademarks, official marks and copyright. Trademarks and official marks are names, logos or other branding associated with an entity. Copyright encompasses a wide range of materials that includes written materials, such as books, manuals, reports and computer software; visual materials such as videos, photographs, pictures, posters and maps; and audio materials such as music and voice recordings.

Like any other type of property, intellectual property can be owned and disposed of by the Province. Disposal of intellectual property involves the sale, transfer or, most importantly in the context of social media sites, licensing of intellectual property rights to third parties. Under provincial policy, unless a ministry has legislative authority or Treasury Board approval to license intellectual property (whether copyright, trademark or otherwise), the approval of the Intellectual Property Program is required.

In relation to copyright-protected materials, where social media sites require a license to materials be provided as a condition of participation, ministries will need to obtain approvals as necessary for pre-existing provincial materials such as documents, videos or photographs. In relation to trademarks or official marks, ministries must not permit any entity to use government logos, branding or marks without approval of the Public Affairs Bureau and, if permission requires a license, approval by the Intellectual Property Program, Treasury Board or ministry legislative authority to license property. The [Disposal Handbook](#) - Chapter 5 - Intellectual Property and Copyright can be found on the [Intellectual Property Program website](#). In addition, prior to posting any copyright-protected materials on a social media site, it is important that ministries confirm that materials posted on the site are owned by the Province and are not encumbered by existing licensing agreements or other terms of use that would prohibit the Province from posting the materials. In relation to trademarks or official marks, ministries must not use the marks of another entity without permission.

Records Management

When information is shared or advice is provided online, government must ensure that all necessary records are being captured, retained, filed and managed appropriately in the office recordkeeping system. If in doubt, discuss the matter with your Records Officer.

Key points:

- If online interactions are [transitory](#) (for example, they do not impact decisions, set policy, or document transactions, and are only for short-term or temporary use) they do not need to be recorded and filed.

Guidelines for Conducting Citizen Engagement, Specific to Social Media

- If interactions are not transitory (for example, they contribute to a decision or policy or are needed to document advice, transactions or operations) they must be recorded. Documentation options include:
 - Creating the record using standard government tools, adding the relevant metadata after posting (e.g. creator/sender, recipient/audience/dates, when and where it was posted) and filing it within the office recordkeeping system.
 - Capturing a copy (e.g. screen shot) of the posting if possible (but only the necessary information as noted in the collection section of the privacy information above) and filing it within your records.
 - Creating a summary or statement of the information communicated and filing that in the office recordkeeping system.

Records management guidelines, fact sheets, records schedules and other resources are available on the [Information Access Operations website](#).

Information Security

When using social media tools, make sure you consider which security settings provided by the site are best suited for your situation and that you understand the terms and conditions of use on the site.

Also, think about your requirements regarding the integrity and availability of information you want to share. Remember, you may be using a site that is not controlled or managed by government. Can you live without the information if the data, or the site, is unavailable for a short period of time, or lost forever? What security controls exist for access to data on the system and will you be able to ensure data provided by one person cannot be altered by another? Will you have the privileges you need to edit, remove or change your postings?

If you have questions or concerns regarding your information security requirements, contact your [Ministry Information Security Officer](#) who can assist you with assessing risks and selecting appropriate security controls. They can also work with you to determine if a Security Threat and Risk Assessment is appropriate for your initiative.

And don't forget, you must immediately report any suspected or actual information incidents (potential or actual breaches of security) to your supervisor or manager, and immediately notify the Office of the Chief Information Officer by calling the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866-660-0811 and selecting Option 3. You will be contacted shortly by the OCIO's Investigations Unit for further details. This procedure is outlined in the [Information Incident Management Process](#).