Office of the
Saskatchewan Information
and Privacy Commissioner

HUMAN RESOURCES POLICY

# 2.0 IPC EXPECTATIONS
# 2.07 INTERNAL SOCIAL MEDIA POLICY

## Purpose

To provide a policy framework that guides the office of the Saskatchewan Information and Privacy Commissioner's (IPC) employees as to the appropriate use of IPC's social media accounts. This policy governs the publication of and commentary on social media by employees of the IPC.

Employees shall refer to IPC Policy 2.04 Information Technology Resources for the overarching IT policy.

## Application

This policy and guidelines applies to all IPC employees, including but not limited to permanent, temporary and student staff.

## Background

### *What is Social Media?*

Social media means any web-based or mobile technology that turns communication into interactive dialogue, including without limitation, blogs, wikis, forums and social networking sites. Examples current to the date of this publication include Twitter, Instagram, Facebook, YouTube and the Saskatchewan Information and Privacy Commission Blog.

### *Risks of Social Media*

Although social media is a dynamic and interactive way to communicate with the public, there are risks associated with participating in social media in an official capacity.

- Online communities offer users anonymity and provide a forum where users can express an opinion to a large audience. As a result, organizations are more susceptible to garnering negative attention when using social media channels. A number of steps can be taken to mitigate this risk, including posting guidelines for users, developing an issues management plan, blocking users, and restricting comment functions.
- Incorrect, and even inappropriate content, can be posted via social media channels. In these instances, the potential for damage is deemed higher for social media than most traditional media because content is often shared instantaneously. While you can correct information and delete a post, it's not necessarily gone for good. For example, if an individual retweets an incorrect message, an organization has no control over that tweet and cannot remove it.
- Given the nature of online communications, audiences may have expectations that the IPC could struggle to meet – in particular, they expect instant replies. In managing an online audience's expectations by responding consistently and in a timely manner, the organization reduces the risks of frustrating, and subsequently losing, users or followers.
- Other risks include staff over-sharing about work through their own personal accounts, engaging in an inappropriate debate with online audiences, or posting content harmful to the organization. These guidelines will address this issue to mitigate the risk.
- Security risks are also an issue because social media sites can lead to increased technological concerns including malware and hacking. It is important to liaise with information technology staff to better understand and reduce these risks.

***Participating as Official IPC Spokesperson***

When participating in social media in an official capacity as an IPC spokesperson we must abide by, but are not limited to, the following:

- Any social media account that is affiliated with the IPC must not conflict with the mission, values and objectives of the IPC; must not contain or link to libelous, defamatory or harassing content; must not reveal confidential or personal information about anyone or work of the IPC related to case files, etc.; must not utilize pseudonyms or false screen names.
- Information (including images, video, etc.) posted on the IPC channels must abide by copyright laws, and must be used only with permission or appropriate citing of the source.
- IPC employees establishing or participating in social media activities as part of his or her official duties must ensure the appropriate approvals have been received prior to engaging. When doubtful think of approvals required for more traditional lines of communication such as letters, emails, media interviews, etc.

The Commissioner reserves the right to shut down any IPC social media channel for any reason at any time.

***Participating Personally***

If you are a staff member of the IPC participating in social media in a personal capacity, be guided by the following:

- Ensure you do not imply in any way that you are authorized to speak on behalf of the IPC. Be clear that you are sharing your personal views and opinions and not the position of the IPC. If you find yourself in a situation where it may be construed that you are acting in capacity as your official role with the IPC, do not engage in the particular topic or forum.
- Any social media identities, logon IDs and user names for social media accounts used in a personal capacity may not include the IPC name.
- Do not take part in any political or public activity which compromises, or might be seen to compromise, your impartial, non-partisan service to the IPC.
- Work time is to be used for IPC business. Blogging and social networking activities are personal and should be done on your own time. Refer to IPC Policy 2.04 Information Technology Resources for further information regarding personal use of IPC IT resources.
- Any information about the work of the IPC, including sensitive job-related information shall not be revealed on social media channels. This includes personal and confidential information.

It is important to remember that there are ramifications to what you publish in a personal capacity, especially when the audience is aware that you are an employee of the IPC. If you are unsure about publishing something and it relates to the IPC do not publish it until you have discussed it with the Commissioner first. You have sole responsibility for what you publish in any form of online social media.

***Protecting the IPC***

When engaging in social media it is important to protect the reputation and integrity of the IPC.

If you are involved with the IPC's social media presence remember that when you post information on a public social media site, you are posting it on the internet and it is public. Once information is in the public domain it can never be completely amended, deleted or retrieved.

- Assume that all information posted on a social media site is insecure, even if you have restricted it to certain users.
- Access, privacy and records management laws and policies apply to social media.
- Do not discuss current or closed files with an individual even if he or she claims that it is his or her own file. Files are only to be discussed through the traditional and accepted forms of verbal (telephone, in-person) or written (email, letter) communication.

***Employee Conduct on Social Media***

Social media is about conversation. It is chatty and informal, but when participating as a representative on the IPC, you must maintain professionalism. You will also need to recognize when a conversation should be taken offline. The internet is forever, so be careful and considerate as the words or conversations can never be fully recovered.

At all times IPC employees must:

- Respect privacy;
- Respect copyright and copyright laws;
- Remain factual and refrain from debates over matters of opinion;
- Avoid responding to negative comments;
- If a mistake is made notify the Commissioner, be upfront and quickly make the necessary correction; and
- Never make partisan or political comments.

**Note:** for more information please see IPC Guidelines for Policy 2.07 Internal Social Media.

## Authority

*The Freedom of Information and Protection of Privacy Act,* section 43.1

## Influencing Sources

Social Media Policy and Guidelines for Citizen Engagement 2014 – Version 2.0 – Government of Saskatchewan
Office of the Information and Privacy Commissioner of Alberta Social Media Guidelines, June 5, 2014
IPC Policy 2.04 Information Technology Resources
IPC Guidelines for Policy 2.07 Internal Social Media