MD of OPPORTUNITY NO. 17
SOCIAL MEDIA AND COMMUNICATION TECHNOLOGY USE POLICY

TITLE: **SOCIAL MEDIA AND COMMUNICATION TECHNOLOGY USE POLICY**

EFFECTIVE:

POLICY NUMBER: **P.9**

PURPOSE OF POLICY

The purpose of this policy is to set out requirements which must be followed by members of the Municipal District of Opportunity No. 17 (MD 17) when communicating through social media and when using communication technology owned or controlled by the MD.

SCOPE OF POLICY

This policy applies to all employees and elected officials of MD 17 and all contractors and external agencies affiliated with MD 17 that Council deems to be subject to this policy; and these entities shall be referred to as "members of MD 17".

CONTENTS

PART 1: SOCIAL MEDIA USE POLICY STATEMENTS

MD 17 supports the use of social media for informational and promotional purposes for the organization, and will promote and support an official presence on social media sites provided the approved communication objectives are met, approved channels are used, and the broader implications and risks in using social media are mitigated.

Authorized Spokespersons

The Chief Administrative Officer (CAO) and his or her designate(s) is the sole authorized spokesperson for the MD with the task of contributing to social media discussions. The Authorized Spokesperson and his/her designate(s) will ensure that:

1. social media posts are identifiable as being made by or on behalf of MD 17;

2. only politically neutral MD 17 positions are conveyed, unbiased by individual personal views;

3. their actions do no harm or potential harm to the reputation of the municipal district;

4. they post information about and for MD 17 only as appropriate to their role; and

5. they remain bound by all MD policies and the *FOIP Act.*

Guidelines for the Authorized Spokesperson

The Authorized Spokesperson and his/her designate(s) will be guided by ALL of the following when posting on social media:

1. Content posted on MD social media channels will be consistent with the goals or objectives of an approved initiative, plan, or strategy.

2. Posts of 'routinely releasable' information (in accordance with FOIP Coordinator categorization) is appropriate for public dissemination;

3. Posts of all other information must be reviewed and approved for publication or dissemination by, at minimum, the FOIP Coordinator, prior to release;

4. Spokespersons are responsible to monitor their social media posts to ensure the posts are effective and maintained;

5. Spokespersons must review "user-created content" such as reader responses to their posts at least once per 48 hours against established and posted (or linked) MD rules of engagement or participation standards;

6. User-create content should be left unmodified, including complaints and criticism, unless the content is "unacceptable," meaning, if it is of a libelous, abusive, hateful, or defamatory character or if it jeopardizes the privacy of others;

7. When user-created content is unacceptable it will be deleted or modified as soon as possible and the spokesperson will make a notation on the social media site identifying that the content was deleted or modified and why;

8. The underlying issue in a user-created complaint, criticism, or question should be identified and responded to as able;

9. Designated Spokespersons must immediately report to the CAO all emergent liability risks such as privacy breaches and grossly negative public relations situations without delay.

Communications Strategy

The CAO and his/her designate(s) will have final approval on the organizational communication strategy and the social media channels used.

To design a communications strategy, initiative, or plan the CAO may utilize a Communications Team which may include the Deputy CAO, the FOIP Coordinator, Information Services staff, and Senior Manager(s).

Risk Management

The use of social media brings risk to an organization. Specific risks include public relations damage, *FOIP Act* breaches, liability, and breaches of copyright / intellectual property law. Risk will mitigated through an assessment of the social media channel(s), including:

1. the reputation and ability of the social media channel(s) to reach the target audience;

2. whether the terms of use of the social media channel(s) will achieve the MD's goals (e.g. to establish a legitimate organizational presence);

3. the appropriateness of posting the intended content to the site;

4. the availability of content moderation and the moderator tools provided by the social media platform;

5. the date or criteria upon which the content and use of the site will be reviewed or discontinued/removed (e.g., after periods of inactivity);

6. the likelihood that MD images, video and other content posted through social media channels can and likely will be downloaded and re-used, altered or re-posted in other ways on other sites;

7. whether residents and visitors have the means to readily and easily access information regarding MD services, programs, facilities without the need to register as a user of the social media site or provide any personal information. Preference will be given to social media channels that permit MD posts to be directly accessible to unregistered users of the channel; and

8. that information and content be made available through multiple social media channels including, at minimum, the MD official website.

Copyright and Intellectual Property Rights

1. Any content placed upon social media sites should be MD-owned or licensed.

2. Content licenses should contain provisions which would allow MD 17 to provide worldwide, fee-free, non-exclusive licenses to third parties in perpetuity.

3. Artists or named personnel whose works may posted to social media sites must be informed in advance of this possibility so that they may waive their copyright and intellectual property rights.

Freedom of Information and Protection of Privacy (FOIP)

Given the risks to privacy posed by social media use, authorized spokespersons will follow these guidelines to protect privacy:

1. A signed release must be obtained from all identifiable persons in a photograph or video before posting, unless the content was obtained during a function where attendees had been notified that photographs or video recordings would be made and disseminated.

2. Use only social media channels having a privacy policy or statement, and a communications reputation that is reasonably compliant with Alberta FOIP or PIPEDA legislation.

3. While members of MD 17 scan or monitor published information available on social media sites, they will not seek to obtain or collect an identifiable individual's personal views, actions, or comments nor take steps to identify the specific author or contributor of published information or content unless authorized and permitted by law to do so.

4. If any official MD content includes personal information, the use and disclosure of that information must be permissible by the *FOIP Act* and specifically reviewed and approved by the FOIP Coordinator.

5. The MD will not collect personal information about individuals who are registered with social media sites unless it is authorized under the *FOIP Act*. In the social media realm, personal information includes an individual's name, email address or username if it includes the individual's name, a portion of their name, or otherwise identifies them.

6. The MD will not use social media as a means of collecting personal information even for specific business purposes. Available web tools or services may be used to obtain ONLY non-identifying anonymous, aggregate or statistical information concerning MD programs, services or marketing efforts from social media sites.

7. All records of MD content posted to, or obtained from, social media sites are subject to the access and privacy provisions of the *FOIP Act*.

Employee Use of Social Media as a Private Citizen

In their capacity as private citizens, MD employees have the same rights of free speech as other citizens. However, they are required as a condition of employment to:

1. Avoid representing the MD in any way on their personal social media sites.

2. Abide by their workplace confidentiality oath and the confidentiality requirements of all MD policy and any other applicable legislation.

3. Never disclose information or content gained through their employment or gathered by MD 17 that they are not specifically authorized to disclose.

4. Understand that content they post or that is posted about them on personal social media sites, if it reflects negatively on the MD, may result in employment disciplinary action. (See the definition of "unacceptable" posts in s.6 of *Guidelines for Authorized Spokespersons*, above, and the Code of Ethics in the MD *Personnel Policy*).

Social Media Use Best Practices

- Never disclose information, including textual or visual content, which is confidential or has been disclosed to MD 17 by a third party.
- Think of what you say in a post in the same way as statements you might make to the media; if you wouldn't say it to a journalist, don't post it.

- Don't cite or reference MD 17 personnel without their approval.
- Be the first to correct your mistakes and report them to your supervisor.
- Ask first: is this post directly related to my area of assigned responsibility?
- Post about timely events. Relevance is important. Update frequently.
- Be prepared and plan ahead to respond to public criticism.

PART 2: COMMUNICATIONS TECHNOLOGY USE POLICY STATEMENTS

"Communication technology" is any means by which information is exchanged between people through a common system, such as computers, monitors, cell phones, telephones, photocopiers, fax machines, software applications, email, internet, intranet, servers, social media sites, radios, and so on.

The MD supports the development of employee and elected officials' capabilities to use communication technology for the purpose of conducting MD business activities. The following requirements apply to all members of the MD organization:

1. Communication devices such as cell phones are critical organizational assets and must be reasonably well cared for. Cell phones damaged to inoperability during their contract period will be replaced once at no cost to the employee; but any subsequent replacement required in the same contract period may require the employee to pay at least 50% of the device cost. Replacement devices will not be upgrades and every replacement is at the sole discretion of the CAO.

2. All information and content created with or stored on municipal communication technology is the property of MD 17 and is a public record subject to disclosure under the FOIP Act, including phone messages, text messages, photos, email, etc.

3. Employees must expect that the MD can and will access any information or content stored on their communication technology at any time regardless of its nature.

4. Employees may not use personal communication technology during work time. Examples include using personal cell phones to make calls, text, view / post on social media, or internet browse. **At minimum, personal cell phones must be stored out of sight during work time;** Senior Managers may, at their discretion, impose additional restrictions on personal devices in departmental work sites.

5. Use of MD communication technology for personal use is permitted as long as it is occasional or incidental and takes place during non-work times or on breaks. Examples include electronic banking, personal research, or flight bookings while on a rest break; educational courses, etc. after hours. The use must not negatively impact the employee's performance or result in damage to the communication technology.

6. The MD reserves the right to track, monitor, audit, and investigate any employee's use of communication technology without notice, including examining text, call, and browsing history; and to limit any employee's access to technology in any way deemed appropriate to his or her position, including limiting or denying internet access.

7. The downloading or streaming of video files using MD communication technology is not permitted except when directly required for employment duties.

8. The installation or download of software onto MD communication technology is not allowed except as authorized and overseen by Information Services staff.

9. Employees must not tamper with or alter any communication technology, and must report operating problems immediately.

10. Use of MD communication technology for campaigns, for-profit ventures, harassment, abuse, illegal or immoral activities, or the perpetration of human rights violations will not be tolerated and can result in immediate termination of employment for cause in addition to prosecution by law enforcement agencies.

ADOPTED November 4, 2015: MOTION #0712-2015-17MDC