



# **WEST MOBERLY FIRST NATIONS**

## **INTERNET, EMAIL, AND SOCIAL MEDIA POLICY**

Adopted:	Sept 29, 2016
Amended:	

## **Objectives:**

- 1) Establish guidelines for West Moberly First Nations (WMFN) employees to conduct Internet use (including email and social media) in both official and unofficial capacities.
- 2) Set expectations and guidelines for Internet use (including email and social media) during working hours.
- 3) Provide a framework for WMFN and employees to use Internet channels to help each other and the community, particularly in the event of a crisis, disaster, or emergency.
- 4) Protect WMFN and employees from violating regulations or laws during use of the Internet (including email and social media).

## **Application and Scope:**

Regular and Casual Employees, Contractors, Chief & Council;

## **Definitions:**

**Employees:** For the purposes of this policy includes regular and casual employees, contractors, Chief & Council.

**Social Media:** The communication channels, tools, and platforms used to create and publish content and interact socially online. Eg: forums, microblogging, social networking sites/apps, social bookmarking, social curation, wikis, etc.

**Spyware:** Software that allows unauthorized people potential access to WMFN passwords and other confidential information.

## **Policy:**

Devices and Internet connections provided by WMFN shall be used for WMFN business only. Devices and Internet connections include (but are not limited to):

- Computers
- Desk phones
- Cell phones
- Tablets
- Laptops
- Desktop computers
- iPads
- Voicemail
- Email
- Social media

Employee-owned devices shall not be used during Regular Working Hours. Except on lunch hours or breaks or as authorized by the Director of Operations or Chief & Council.

## **I. Confidential Information**

- 1) WMFN confidential information shall not be shared outside of WMFN, without authorization, at any time. This includes information about WMFN that has not been publicly released; information that concerns other employees, members, community members, or WMFN operations; and proprietary WMFN information. This is true regardless of employment status; ie: past, present, or on leave.
- 2) Questions regarding WMFN information shall be referred to the Director of Operations prior to releasing information that could potentially harm WMFN and/or WMFN affiliates. The Director of Operations shall refer to Chief & Council for situations requiring Chief & Council authorization. For more information, please refer to WMFN Human Resources Policy: Confidentiality.
- 3) Employees who disclose confidential information will be disciplined, up to and including immediate termination or legal action.

## **II. Harassment and Bullying**

- 1) Bullying or content that discriminates against any protected classification including age, race, color, religion, sex, weight, sexual preference, national origin, disability, or genetic information is prohibited.
- 2) WMFN owned electronic equipment, including devices owned by the employee, shall not be used on WMFN time, to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related Internet sites. Please reference Sexual Harassment definition in WMFN Bullying and Harassment Policy.
- 3) Participation in the above activities will result in disciplinary action up to and including termination of employment. For more information, please refer to WMFN Human Resources Policy: Bullying and Harassment.

## **III. Legal Liability**

- 1) Employees are legally liable for anything they write or present online. Employees shall be disciplined by WMFN for any commentary, content, or images that are defamatory, pornographic, proprietary, bullying, harassing, or libelous. This applies to any and all content created or stored on WMFN equipment/databases (See WMFN Bullying and Harassment Policy).
- 2) WMFN owns all communication that is stored on WMFN equipment. This includes but is not limited to email communications and browsing history. Management and other authorized staff have the right to access any material on WMFN equipment at any time. Employees shall not consider electronic communication, storage, or access to be private if it is created or stored on WMFN equipment or systems.
- 3) Inappropriate activity that is in conflict with this policy may result in termination for just cause. Further, WMFN will report unlawful activity to the authorities.

#### **IV. Software and Equipment**

- 1) Only individuals with authorization from the Director of Operations shall use the Internet to access software additional to that which is generally approved for all employees.
- 2) Upon leaving WMFN employment for any reason, any and all WMFN equipment and associated information shall be returned on the last day of work.
- 3) Any and all WMFN equipment provided for public use must be used in accordance with this policy. Misuse of equipment includes:
  - Streaming video (unless authorized by the Director of Operations)
  - Downloading (images, video, documents, programs, applications, etc.) (unless authorized by the Director of Operations)
  - Defamatory content
  - Harassment or bullying of any kind, regardless of relation to WMFN

#### **V. Internet Usage**

- 1) West Moberly First Nations (WMFN) recognizes the importance of the Internet in shaping public opinion about WMFN and current and potential businesses, employees, industry partners, and departments.
- 2) Writing about or displaying internal WMFN happenings, including photos, videos, and comments, shall not be allowed without pre-written permission from the Director of Operations and a signed release when required (photos and videos). The Director of Operations shall refer to Chief & Council for situations requiring Chief & Council authorization.
- 3) Inappropriate content including but not limited to copyrighted materials, unfounded statements, or derogatory content will result in disciplinary action up to and including termination of employment.
- 4) WMFN at its sole discretion, reserves the right to block access to any Internet site.
- 5) Employees shall make every possible attempt to avoid breaches to the security of confidential WMFN information as well as contamination to the WMFN system via viruses or spyware.
- 6) All email use during working hours shall be for WMFN business. WMFN email addresses shall be used for WMFN business only. Employees shall not use personal email addresses for WMFN business.

## VI. Social Media

- 1) WMFN recognizes the importance of our employees' assistance in attracting quality employees, improving WMFN reputation, and shaping industry conversation and direction through blogging and interaction on social media sites (e.g. Facebook, LinkedIn, Google+, Wikipedia, Instagram, Twitter, LinkedIn, Wordpress, and YouTube). Therefore, WMFN is committed to supporting employees to interact knowledgeably and socially on the Internet and social media sites both at work and in the privacy of your own home.
  - a) **Note:** *This policy does not apply to employees' personal use of social media platforms outside of work-hours where the employee uses personal equipment, makes no reference to WMFN or WMFN related topics, and does not violate the Harassment and Bullying Policy.*
- 2) Before engaging in work-related social media, employees shall obtain the permission of the Director of Operations. As well, social media identities, logon ID's, and user names shall not use WMFN's name or logo without prior approval from the Director of Operations.
- 3) Employees shall submit a proposal to the Director of Operations prior to developing any official program or department social media or internet site. This proposal shall include:
  - Department/project the site will be developed for
  - Purpose of site (e.g. communication, stakeholder consultation, forum, etc.)
  - Identification of site administrator
  - Identification of site moderator if comments will be enabled
  - Moderation rules/policy.
- 4) WMFN expects employees to exercise personal responsibility when using social media, which includes not violating the trust of those with whom they are engaging. Employees shall not use social media for political lobbying, marketing, or public relations. If and when employees use social media to communicate on behalf of WMFN, they shall clearly identify themselves as employees.
  - a) **Note:** *Examples of appropriate and inappropriate use of social media can be found in Appendix 1*

## VII. Personal Use

- 1) Any employee developing content (eg: a web site, blog, or other social media page) that will mention WMFN and/or its affiliates shall inform the Director of Operations. Additionally, the employee shall disclose in said content their identity as an employee of WMFN and that the views expressed belong to said employee and do not represent the views of WMFN.
- 2) Any personal content shall not violate the Confidential Information section of this policy. This includes sharing information about WMFN that has not been publicly released; information that concerns other employees, members, community members, or WMFN operations; and proprietary WMFN information. Employees who disclose confidential information will be disciplined, up to and including immediate termination or legal action.
- 3) Further, WMFN websites, forums, and social media pages/accounts/groups shall not be used for political lobbying. The sole exception is employees authorized by the Director of Operations to lobby on behalf of a WMFN initiative on a provincial, federal, or international issue.

- 4) Personal use of social media that is in conflict with this policy will result in disciplinary action up to and including termination of employment.

**REVIEWED & RECOMMENDED**

This WMFN Internet Email and Social Media Policy has been reviewed and approved by a quorum of Council on [September 29, 2016], coming into force on [September 29, 2016]:

Councillor: Patricia Brown

Councillor: Dean Dokkie

Councillor: Robyn Fuller

Councillor: Clarence Willson

This policy has been reviewed and amended by a quorum of Council:


**Note:** *This appendix provides examples only. It does not express all proper uses or misuses of social media. Any questions or concerns regarding the use of social media shall be referred to the Director of Operations.*

Proper use of social media:

- Post meaningful, respectful comments - no Spam and no remarks that are off-topic or offensive.
- Stick to your area of expertise and feel free to provide unique, individual perspectives on non-confidential activities at WMFN.
- Represent yourself or WMFN in a truthful way. All statements must be true and not misleading; all claims must be substantiated
- The privacy settings on social media sites shall be set to allow only information similar to the displayed on the WMFN website.

Misuse of social media:

- Comment on any topic related to legal matters, litigation or any parties WMFN may be in litigation with.
- Participate in Social Media when the topic being discussed may be considered a crisis situation. Even anonymous comments may be traced back to your or WMFN's IP address.
- Political Lobbying
- Defamatory/derogatory comments about management or leadership