Rationale

Employees have access to e-mail and internet accounts in order to meet the First Nation Land Management Resource Centre’s (“Resource Centre”) business requirements. All use of the Resource Centre’s facilities and equipment shall be done in a manner which retains the integrity and professionalism of the Resource Centre as well as the integrity of the Resource Centre’s computer facilities and equipment.

The rapidly growing phenomenon of user-generated web content such as blogging, social web-applications and networking, are important arenas for communications, employee engagement and learning. This policy provides practical guidelines to employees when participating in online social media activities and is in no way intended to inhibit or prevent employees from expressing their personal views when engaging in social media for personal use.

Application

This policy applies to all employees, Board members, volunteers, consultants and contractors of the Resource Centre and the use of “employees” is to be read broadly in this regard. This policy also applies to employees using social media for work purposes and to the personal use of social media when away from work when the employee’s employment is identified, known, or presumed.

This policy also applies to:

(i) all computer and data communication systems, facilities and equipment owned by and/or administered by the Resource Centre;
(ii) stand-alone desktop computers with dial-up or wireless modems as well as those attached to networks;
(iii) personal devices used for Resource Centre business.

Definitions

“Devices” includes but is not limited to smartphones, tablets, computers and laptops.

“Facilities and equipment” includes but is not limited to computers, laptops, servers, computer systems, software, hardware, the network and other equipment that the Resource Centre may make available to employees.

“Social media” includes, but is not limited to, blogs, personal websites, podcasts, discussion forums, online collaborative information and publishing systems such as Wikis, photo sharing services such as Flickr, video sharing services such as YouTube, social networks like MySpace and Facebook as well as micro-blogging services such as Twitter.

Policy

(i) No reasonable expectation of privacy

Employees shall have no reasonable expectation of privacy in their use of the Resource Centre’s computer facilities and equipment. Employees are reminded that the Resource Centre has the right to review an
employee’s computer use, including monitoring e-mail and internet access. Employees who want their communications to remain private should not utilize the Resource Centre’s computer facilities or equipment for such private communications.

(ii) Email Etiquette

Employees are reminded that when sending or receiving e-mail from the Resource Centre’s facilities, they are identified as an employee of the Resource Centre. All e-mails shall comply with appropriate “netiquette” and should be consistent with the Resource Centre’s reputation, standards and other workplace rules. Copies of business e-mails sent and received shall be maintained in appropriate files.

(iii) Bona Fide Business Use

Computer facilities and equipment are to be utilized for bona fide business purposes. While the Resource Centre acknowledges that employees may send or receive an occasional personal e-mail or utilize the internet for personal matters on an incidental basis during breaks and before and after working hours, it is expected that employees will act responsibly and in the best interest of the Resource Centre when using our facilities and equipment. Incidental personal use must not interfere with the performance of employees’ duties.

(iv) Unacceptable and Prohibited Uses

Unacceptable use of the Resources Centre’s computer facilities and equipment include the following:

(i) using the facilities and equipment in conflict with our objectives, such as to operate a personal business or to seek alternate employment;
(ii) broadcasting personal points of view such as commentaries on social or political issues;
(iii) participating in internet chat groups;
(iv) using the facilities and equipment to buy or sell items; and
(v) using the facilities and equipment to participate in on-line games.

Employees shall not use the Resource Centre’s computer equipment and facilities for any illegal, unethical or immoral purposes. For example, the Resource Centre’s facilities and equipment shall not be used to access child pornography, obscenity or hate literature and shall not be used to transmit defamatory, derogatory or false messages.

Employees shall not share personal information concerning themselves or their co-workers via the internet. Internet and e-mail access shall not be utilized to communicate any confidential or sensitive commercial information unless prior approval is obtained from the Executive Director or designate.

Employees shall not download software from the internet unless prior management approval is obtained. Employees are not to participate in any use of the computer system which might infringe copyright, other intellectual property rights or licensing agreements.

Employees shall not utilize the Resource Centre’s facilities and equipment in a manner which may compromise the integrity of the system or the systems performance. Employees shall not open any attachment where the source is suspect. All e-mail attachments shall be checked to ensure that they remain free from viruses before they are opened or downloaded.

The Resource Centre assumes no responsibility or liability whatsoever for any unauthorized use of software, information or materials sent, received or transmitted through the internet or e-mail.
(v) **Email Guidelines**

The following forms of email, other than in the proper and authorized course of business, are prohibited using your Resource Centre email address: chain mail; mass mail; advertising or soliciting (including charities); impersonating another user; harassing mail; any mail in which the content would violate any Resource Centre policy; threats. The use of anonymous “re-mailers” or other methodologies to conceal one’s identity when sending email is prohibited.

Employees are reminded of the obligations contained in the Canadian *Human Rights Act* and the workers’ right to freedom from discrimination and harassment in employment. Employees shall not access or download material which might reasonably offend their co-workers or send, store or transmit offensive, objectionable, pornographic, obscene, sexist, racist or provocative messages. Employees are reminded not to send threatening or demeaning messages or to circulate jokes which might reasonably offend a co-worker. Employees should refer to the Respect in the Workplace Policy for further information as to what constitutes harassment.

(vi) **User I.D. and Passwords; Access to Accounts**

All employees are responsible for activity which takes place using their user I.D. and password. Employees shall not provide any other individuals with their user I.D., password, or access to their computer account, including e-mail and internet accounts, unless prior approval is obtained by the Executive Director or designate. Such approval shall be granted in exceptional circumstances only.

Employees shall not access another user’s internet or e-mail account without the approval of the Executive Director or designate, save and except where the Resource Centre is monitoring employees’ computer usage for the purpose of enforcing this policy.

(vii) **Monitoring, Access, Use**

The Resource Centre reserves the right to monitor e-mail and internet use to ensure compliance with this Policy. Employees are advised that the Resource Centre may, in its sole discretion and without further notice to employees, intercept, retrieve, access, review, disclose and use any communications and/or activity, including internet access and e-mail for the following purposes:

(i) there is a request for a document which must be produced for the purposes of litigation or other similar types of proceedings;  
(ii) to monitor excessive recreational use while employees are at work and/or using systems provided by the Resource Centre;  
(iii) to engage in technical maintenance, repair and management;  
(iv) to ensure continuity of work processes;  
(v) to improve processes and manage productivity;  
(vi) there is a business need;  
(vii) the Resource Centre has reason to believe that the computer network is being used in violation of this Policy or the law; or  
(viii) to investigate a breach of an employment contract or policy.

(viii) **Resource Centre Property**

All messages, files, documents and other information generated by employees using the resources of the Resource Centre are the property of the Resource Centre. Resource Centre facilities and information
should only be used for business purposes and as specifically permitted by the Executive Director or designate.

(ix) Social Media

Employees may be members of social networking sites or may engage in other online chat groups, blogs, etc. Employees are prohibited from identifying themselves as employees of the Resource Centre when posting comments on the internet or on other online services. Internet traffic sent via the Resource Centre’s facilities and equipment is generally identifiable as being from an employee of the Resource Centre; participation in internet newsgroups and the like using the Resource Centre’s equipment or facilities is therefore prohibited.

Employees understand and agree that, in engaging in social media activities, they must comply at all times with their workplace obligations, including but not limited to obligations in regard to loyalty and confidentiality, as well as with respect to all human rights policies, guidelines and applicable legislation.

Using Social Media for Work

Employees shall not disclose confidential or proprietary information or similar information of third parties, including but not limited to member First Nations who have shared such information with the Resource Centre. The Resource Centre’s intellectual property, trademarks, and copyrights shall not be used in any manner without the approval of the Resource Centre.

The Resource Centre reminds all employees that the Code of Conduct must be respected while participating in blogs, online discussion forums or any other social media activities. All employees are to represent the Resource Centre in a professional and business-like manner as would be expected in any other public forum or medium, and should exercise discretion, thoughtfulness and respect for colleagues.

Employees must ensure that they have all the facts before posting information to avoid having to post a correction or a retraction. Should an error occur, it should be corrected quickly and visibly.

Employees are not permitted to use the Resource Centre’s social media channels for which they have login credentials for self-promotion or the promotion of their own personal business or creative projects.

Personal Use of Social Media

The following is a non-exhaustive list of requirements when employees are using social media for non-work purposes:

- Do not share photos or personal information about colleagues, Board members, First Nations or anyone else with whom the employee has come into contact with in the course of employment with the Resource Centre;
- Do not share any confidential business information of any kind, including computer passwords, security information, ID information, or any other information obtained in the course of employment.

Employers, including the Resource Centre, have the ability and the right to monitor social media sites. Employees who post information that adversely impacts the business interests of the Resource Centre, breaches confidentiality or irreparably undermines their employment relationship will be disciplined up to and including termination of employment.
Individuals are legally liable for what they post on their own site(s) and on the sites of others. Individual bloggers can be held liable for commentary deemed to be proprietary, copyrighted, defamatory, libellous or obscene (as defined by the courts).

(x) **Personal Devices**

An employee may use their personal device(s) in the performance of their job duties on the understanding that the use of a personal device in connection with the Resource Centre’s business is a privilege granted to employees through approval of management. Employees are not permitted to use personal devices without having obtained the advance written permission of the Executive Director or designate. The Resource Centre reserves the right to revoke the privilege at any time and for any reason. Users of personal devices for Resource Centre business must agree to all terms and conditions in this Policy to be permitted access to the Resource Centre’s networks. The Resource Centre reserves the right to disable or disconnect some or all of its remote services without prior notification to employees.

Users of personal devices are responsible for keeping their devices current and this includes, but is not limited to, ensuring the device has all recent security, software and firmware updates. Any device which is used to access Resource Centre systems and/or networks must be equipped with a password lock. Only Resource Centre employees will be permitted to access our data on personal devices. Should the employee lose or report their personal device stolen, the Resource Centre must be notified as soon as possible to prevent unauthorized access to the network from the missing device. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

As a condition of using personal devices for Resource Centre business, employees consent that the Resource Centre may intercept, access, retrieve, read, disclose, and use any telephone or voice mail communications and/or computer systems activity, including Internet access and electronic mail, on a personal device, for the same purposes as set out in section (vii) above.

In using their personal device to fulfil job functions, the employee recognizes that they have a diminished expectation of privacy with regards to their personal device.

**Violations of this Policy**

Any violations of this Policy, in whole or in part, may result in disciplinary action which may include, but not be limited to, termination of employment or contract and/or such other legal actions as may be warranted in the circumstances.