SECTION II – ESSENTIAL ORGANIZATIONAL POLICIES

CATEGORY: Essential Organizational Policies	**NUMBER: 2.12**
SUBJECT: Telecommunication and Technology	**PAGE: 40**
APPROVED: November 2009	**REVISED:**
ANNUAL REVIEW DATE: Fall 2011 Reviewed January 2016	

PURPOSE

To establish telecommunication and technology policies and procedures by which employees, independent contractors, participants, volunteers and others safeguard the reputation and integrity of WSNCC.

POLICY

Users must respect the integrity of WSNCC and its affiliates by following protocols and procedures for use of technology, email and internet platforms.

The telecommunication and computer systems belong to the organization and may be used only for business purposes, at the discretion of the WSNCC.

Only the Administrator adds new programs or software to computers.

Unauthorized sending, transmitting or otherwise disseminating proprietary data, trade secrets or other confidential information of the company is strictly prohibited may result in substantial civil liability as well as severe criminal penalties under the law.

Users shall not intentionally develop or use programs that harass other users or infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.

Employees are not authorized to engage in any activity that is illegal under local, provincial, federal or international law while utilizing equipment or resources owned by WSNCC or its affiliates.

PROCEDURES

1. Users should not have an expectation of privacy in anything they create, store, send or receive on the computer or phone system.

2. Telecommunication and computer systems may be used only for legitimate purposes to assist in the performance of various jobs designated by WSNCC and its affiliates. Use of the computer system is a privilege that may be revoked at any time.

3. Staff and users must obtain prior written permission from senior management or the Executive Director for the dissemination or storage of information which is unauthorized or non-work-related but of potential benefit to the organization.

4. Staff may only connect to other computer systems through the network or by a modem and make use of those systems if specifically authorized by the operators of those systems and senior management or the Executive Director.

5. Staff and users will report uses that waste Telecommunication or Computer Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, having extended personal calls, printing multiple copies of documents or otherwise creating unnecessary communications or network traffic.

6. Prior written authorization must be obtained from the senior manager or Executive Director to do any of the following:
   i. copy software for use on home computers;
   ii. provide copies of software to independent contractors, third parties or clients of WSNCC;
   iii. install software on any of WSNCC and affiliates workstations or servers;
   iv. download software from the Internet or other online service to WSNCC workstations or servers;
   v. modify, revise, transform, recast or adapt any software;
   vi. reverse-engineer, disassemble or decompile any software unless any of these provisions are required as part of the job-description.

   Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisors.

6. From time to time resident software may be located on a temporary or permanent basis on any or all computers within the WSNCC and/or affiliates system. This software may be for monitoring purposes of individual computer systems for performance reasons and is placed there at the discretion of WSNCC and may not be tampered with for any reason. Anyone discovered tampering with any installed software, removing said software or modifying said software without express consent will be liable for disciplinary action, up to and including dismissal.

7. Each User is responsible for ensuring that use of outside telecommunications, computers and networks, such as the Internet, does not compromise the security of WSNCC Computer Resources. This duty includes taking reasonable precautions to prevent intruders from accessing the company's network without authorization and to prevent introduction and spread of viruses.

8. Each user is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into WSNCC network. To that end, all material received on disks or other magnetic or optical medium and all material downloaded from the Internet or transferred from computers or networks that do not belong to WSNCC must be scanned for viruses and other destructive programs before being placed onto the computer system.

9. Printers and photocopiers are to be used to effectively conduct business, service and program activities/functions as required by WSNCC and other uses must have the approval of senior management or the Executive Director.

10. Staff and users will report the unlawful use of material through telecommunication and computer systems to senior managers or the Executive Director.

PLEASE NOTE:
This Policy applies to ALL means of communication, being it verbal and/or written, in person and/or by telephone, fax, e-mails, texting, instant messaging, social networking sites (i.e. Facebook, Twitter, My Space etc.) and any other current and future forms of communication and information technology.