Electronic Equipment Use Policy – Six Nations of the Grand River Elected Council

Category: Governance	Date for Review: December 10, 2027
Approved By: ICPL#419/12/09/2024	Previous Version: GC#699/09/07/2010
Effective Date: December 10, 2024	

1. Purpose

1.1 Members of Council utilize Six Nations of the Grand River (SNGR) owned Electronic Equipment to conduct the daily business of Council. However, the costs of Electronic Equipment and the risk of unlawful or damaging actions are high. Thus, proper controls need to be in place to provide guidance regarding proper use of the Equipment, including the data stored on the equipment itself and address issues of the costs associated with provision, installation, and operation.

2. Policy Statement

2.1 This policy's intent is to provide greater clarity to Members of Council when using SNGR owned Electronic Equipment and governs the use of Council's information technology and all information and communications sent, received, through and stored on SNGR owned Electronic Equipment. Members of Council who utilize SNGR owned Electronic Equipment shall abide by the following provisions contained herein, or otherwise may be subject to disciplinary action or referral to the appropriate legal authorities for failing to comply.

3. Definitions

3.1 **Council or Members of Council or SNGREC**- means the Elected Chief and Elected Council Members, not including employees.

3.2 **Electronic Equipment** –means all technology resources which includes computer and communications equipment installed on SNGR property or otherwise furnished by SNGR, whether individually controlled or shared, stand-alone or networked, and

whether owned, leased, operated, or controlled by SNGR, and including but is not limited to:

(a) networking devices,

(b) cellular telephones, iPads, and

(c) any associated peripherals and software regardless of its purpose

3.3 **SNGR** – means Six Nations of the Grand River. Six Nations of the Grand River is the legal name of the Elected Council and the organization as a whole which includes employees.

3.4 **SNGREC** – means Six Nations of the Grand River Elected Council.

3.5 **Third-Party Connections**- means vendors, contractors, consultants and external entities.

3.6 **User(s)** – means the Elected Chief and Elected Council Members, not including employees.

4. Scope

4.1 This policy applies to all SNGR owned Electronic Equipment used by Members of Council.

5. Legal Compliance

5.1 All users of SNGR's information systems must comply with all federal, provincial, and other applicable law; all applicable Council rules and policies, including, but not limited to those which apply to personal conduct and those specific to computers and networks; and all applicable contracts and licenses.

5.2 Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

5.3 All users are cautioned that any electronic correspondence (e-mail, text messages etc…) may be subpoenaed and used as evidence in legal proceedings.

6. Authorized Uses

6.1 All users of SNGR's information systems shall use only those electronic resources that they are authorized to use and use them only in the manner and to the extent authorized.

6.2 Members of Council shall identify any correspondence of a personal nature that uses Council property which incurred a cost that is not ordinarily covered by the organization.

6.3 Except where permitted by Voluntary Disclosure (VD), Internet use shall be for work related research purposes only.

6.4 Electronic Equipment that is utilized during a meeting, or during other Council business, shall only be used for legitimate, business-related purposes.

6.5 Members of Council shall be entitled to internet access at their homes. The cost of such access shall not exceed eighty dollars ($80.00) monthly.

6.6 Members of Council shall be personally responsible to pay for any cost incurred due to personal, non-business-related use of SNGR owned Electronic Equipment.

6.7 Ability to access computing resources does not, by itself, imply authorization to do so.

6.8 Users are responsible for ascertaining from Information Technology Solutions what authorizations are necessary and for obtaining them before proceeding.

6.9 Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by SNGR.

6.10 Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information violate SNGREC’s policy and may violate applicable law.

6.11 All users must use systems and resources in ways that do not interfere with or disrupt the normal operation of these systems, nor interfere with the access and use of these systems and resources by others allowed to do so.

7. Prohibited Conduct

7.1 Harassment and Bullying

7.1.1 No user may, under any circumstances, use SNGR’s computer systems or networks to libel, slander, threaten, bully, or harass any other person.

7.2 Capacity Used

7.2.1 All users of SNGR’s information systems shall respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to unreasonably interfere with the activity of other users.

7.2.2 Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of SNGR's computing resources, Council may require users of those resources to limit or refrain from specific uses in accordance with this policy.

7.2.3 The reasonableness of any particular use will be evaluated at the discretion of SNGREC in consultation with Information Technology Solutions, who shall take into consideration all of the relevant circumstances.

7.2.4 Users must be good stewards of the electronic equipment, system and network resources offered by SNGR. Examples of poor stewardship include but are not limited to: excessive personal use; streaming services i.e. Netflix, Disney, Prime, etc.; game playing; continuous running of background programs and reception of large files or running intensive multimedia network applications (digital/internet radio or other media), use of unauthorized flash and portable flash drives or accessing any form of explicit or illegal material.

7.2.5 Users rely on shared computing and networks simultaneously and, therefore, each user must consider the needs of other users when using these resources.

7.3 Illegal File Sharing

7.3.1 Copyright abuse can subject both the user and SNGR to legal sanctions. Sharing copyrighted materials without a license (i.e., Peer-2-Peer [P2P] file sharing which is often automatically shared) is against the law and also prohibited under this policy. Any individual found to be participating in illegal file sharing will be subject to disciplinary action.

7.3.2 Federal law requires SNGR to take action when it is notified that someone on its network is distributing copyrighted materials. SNGR will not protect any individual users, who distribute copyrighted material without license, nor will it protect or defend individuals who have improperly used SNGR owned Electronic Equipment, system and/or network resources.

7.4 Personal Gain or Benefit

7.4.1 All users shall refrain from using SNGR information systems resources for personal commercial purposes or for personal financial or other gain.

7.4.2 All users shall refrain from seeking personal benefit or permit others to benefit personally from any confidential information that has come to them by virtue of being an elected official.

7.4.3 Personal use of SNGR computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other Council responsibilities, and is otherwise in compliance with this policy.

7.4.4 Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

7.5 Software License Abuse

7.5.1 SNGR requires strict adherence to software vendors' license agreements. Copying of software in a manner not consistent with the vendors' license is strictly forbidden on SNGR owned Electronic Equipment, system and network resources.

7.6 Damage to Equipment

7.6.1 It is the responsibility of a user to ensure that Electronic Equipment is maintained in a state of good working order and is stored in a secure manner at all times and not left unattended in public spaces.

7.6.2 No person, other than those authorized to do so, shall operate Electronic Equipment belonging to SNGR.

8. Privacy

8.1 All users of SNGR’s information systems shall respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Ability to access other persons' accounts does not, by itself, imply authorization to do so.

8.2 Users should be aware that their uses of the SNGR computing resources are not completely private. Users are also cautioned that computer use may be monitored. The

normal operation and maintenance of SNGR technology resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service.

8.3 SNGR may also specifically monitor the activity and accounts of individual users of SNGR technology resources, including individual login sessions and communications, without notice, when:

(a) The user has voluntarily made them accessible to the public;

(b) It reasonably appears necessary to do so to protect the integrity, security, or functionality of Council or other computing resources or to protect SNGR from liability;

(c) There is reason to believe that the user has violated, or is violating, this policy or any Council related policy;

(d) An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or

(e) It is otherwise required or permitted by law or for any other legally permitted reasons associated with the evaluation, testing, repair or general operation of the SNGR owned Electronic Equipment resources.

8.4 SNGR, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate SNGR personnel or law enforcement agencies and may use those results in appropriate Council disciplinary proceedings.

8.5 Authorized system administrators from Information Technology Solutions may access computer users' files at any time for maintenance purposes. System administrators from Information Technology Solutions will report suspected unlawful or improper activities to the proper authorities.

9. Security

9.1 SNGR employs various measures to protect the security of its technology resources and of their users' accounts. Users must be aware, however, that SNGR cannot guarantee such

security. Users should therefore engage in "cybersecurity" best practices by establishing appropriate access restrictions for their accounts and guarding their passwords.

10. Additional User-Specific Provisions

10.1 Website Reproduction

10.1.1 In addition to fully complying with this policy's general provisions identified in sections 1 through 11, inclusive, personal websites are not to be housed on SNGR's web servers.

10.1.2 In addition, all SNGREC information that a Council member desires to post on their personal websites should be done in a manner that abides by the Code of Conduct for Members of Council Policy and the 2023 SNGR Election Code.

10.2 Third-Party Connections to the SNGR Network

In addition to fully complying with this policy's general provisions identified in sections 1 through 11, inclusive, all third-party connection users are subject to the following additional provisions:

10.2.1 Users shall protect the security of SNGR systems, the confidentiality and privacy of SNGR employees and records.

10.2.2 All Electronic Equipment resources and equipment must be inspected by Information Technology Solutions. The inspection is intended to verify that the appropriate level of security is in place, as well as verify the existence of proper communication equipment, technical settings, hardware compatibility and anti-virus protection.

10.2.3 Any equipment deemed insufficient or a risk to the SNGR network may be denied access until deemed acceptable.

10.2.4 Any external equipment and network devices not made available for the inspection may be disconnected from the SNGR network until proper inspection is completed.

10.2.5 If any equipment or network device is suspected of endangering network health, performance or security is subject to immediate disconnection.

10.2.6 Any intrusive security audits or tests which may impair the connectivity, functionality and health of the SNGR network must be scheduled and approved by Information Technology Solutions in advance of any such audit or impairment.

11. Enforcement

11.1 All users of SNGR owned Electronic Equipment resources who are found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to: warnings, reprimand, suspension, removal of Electronic Equipment privileges and/or legal action.

11.2 Any alleged violations of system abuse shall be referred to the Integrity Commission for determination.

11.3 All users, when requested, are expected to cooperate with system administrators in any investigation of system abuse.

11.4 Users are expected to report suspected abuse, especially any damage to or problems with their files.

11.5 Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.

11.6 Council Members should be aware that e-mail on their SNGR account and files on SNGR computers may be subject to public disclosure.

11.7 Further, SNGR reserves the right to access e-mails and files on Council computers when needed for work-related purposes.

11.8 SNGR may temporarily suspend or block access to an account prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of SNGR computing resources or to protect SNGR from liability.

11.9 SNGR may also refer suspected violations of applicable law to appropriate law enforcement agencies.

12. Authorization

12.1 This policy was approved by Six Nations Elected Council at the General Council meeting held on September 7, 2010 by resolution No. GC#699/09/07/2010 to be effective on December 7, 2010.

12.2 Amendments to this policy must be approved by a Council Resolution.

12.3 This policy replaces the Six Nations' Council Electronic Equipment Use Policy approved by SNCR No. ICPL#50/27/10/2008.

12.4 This policy was amended and approved by the Six Nations of the Grand River Elected Council at the Political Liaison meeting held on December 9, 2024, by resolution ICPL#419/12/09/2024 to be effective on December 10, 2024.