Tsawwassen First Nation
Information & Technology Management Policy

September 2008

Table of Contents

Introduction

Information and technology are tools that play a key role in supporting the Tsawwassen First Nation's business and assisting staff in performing their job duties. When planned and managed properly, they can also improve productivity and reduce costs.

Information technology (IT), as it is used in this policy, refers to anything related to computing technology, such as networking, hardware, software and the Internet - and includes the full spectrum of technologies and services that support the management of information in an electronic form.

This policy is the central resource for policies and procedures related to the use, management and security of IT at TFN.

1. Appropriate Use of TFN IT Systems and Equipment

It is the responsibility of every staff person to ensure TFN's information and technology systems are properly managed, secure and used only for authorized purposes and in accordance with TFN policies. It is the objective of this section to outline, in general terms, what is expected of TFN employees in relation to information and technology. The misuse and mismanagement of information and technology could have negative impacts for the TFN organization at large. Therefore, employees who fail to comply with these standards may be subject to disciplinary action up to and including dismissal.

1.1 Disclosure of Private & Sensitive Information

TFN's IT systems and resources must not be used in ways that could improperly disclose confidential, sensitive, or proprietary information to unauthorized individuals or in violation of federal, provincial or local law.

1.2 Honesty & Integrity

TFN employees must conduct themselves honestly and appropriately while using TFN's IT systems and when on the Internet for job-related duties. Employees are expected to respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as in any other business dealings. They must also not misrepresent their identity as senders of messages nor the content of such messages.

1.3 Protection of TFN's Reputation

TFN employees should always be aware that transmissions accomplished using Internet addresses and domain names registered to TFN may be perceived by others to represent the organization. TFN staff are advised not to use the Internet for any purpose that would reflect negatively on the TFN.

1.4 Security Protection

Employees are required to take all necessary precautions to: preserve the privacy of data to which they have access, respect the privacy of others by not tampering with e-mail, files, or accounts they use; and respect the integrity of computing systems and data.

1.5 Personal Use

Access to the Internet should be related to TFN job-related duties.

Computer IDs, accounts, and other information and technology systems and resources are to be used for authorized purposes. Use of TFN resources such as computers or network capacity for personal use of the Internet ("browsing") is prohibited during working hours. Staff are to limit personal use of the Internet to the hours before or after work, or during lunch or break times.

Unauthorized access to networks, computers or databases is also forbidden.

Equipment that has been supplied by TFN for staff use remains TFN property.

1.6 Examples of Inappropriate Use

The following are some examples of what would be considered unacceptable uses of the TFN's information and technology systems and resources:

- Attempting to guess a password or gain unauthorized access to remote computers.
- Attempting to monitor or read files or communications without proper authority.
- Using abusive or offensive language in any electronic communications associated with TFN.
- Obtaining unauthorized access to networks, computers or databases.
- Deploying TFN IT systems to gain illegal or unauthorized entry to another person's or organization's computer/system.
- Using TFN information and technology resources for commercial activities unrelated to the business of TFN.
- Using IT resources in a way that disadvantages other users, (i.e. streaming/listening to audio, watching videos over the internet or downloading of large files) except where such activity is directly related to the business of TFN.
- Altering or copying of system software licensed to TFN without approval of the IT Department.

- Exposing TFN's information and technology systems to unlawful information, computer viruses or other harmful programs in the form of either public or private files.

1.7 Reporting Possible Illegal and Unacceptable Use

TFN employees are expected to report to their Department Manager all suspected illegal or unacceptable use of TFN information technology resources.

2. Privacy and Security

This section is intended as a guide to provide for the protection of personal data, systems, documentation, computer-generated information and facilities from accidental or deliberate threats to confidentiality, integrity or availability. Security policies apply to all locations where information is processed or stored by, or on behalf of the TFN, whether that is on site or through remote access. IT security is the responsibility all council members, managers, employees, contractors and others who have access to, use or manage the information and technology assets of TFN government.

2.1 Private and Confidential Information

All data collected by TFN employees or contractors must be used only for the purpose for which it was originally collected.

Confidential information that TFN employees receive through their employment must not be divulged to anyone other than persons authorized to receive the information.

Confidential information must also not be used by employees for the purpose of furthering any private interest, or as a means of achieving personal gain.

Employees who are in doubt as to whether certain information is confidential must ask their supervisor before disclosing it.

2.2 Information Storage

Information and operational data should be stored on designated network drives, such as the departmental drive or the personal drive. This ensures data protection, integrity, and allows for business continuity.

2.3 Intellectual Property Rights of Others

TFN employees are expected to respect the rights of others by complying with all TFN policies regarding intellectual property regardless of medium (i.e. paper or electronic). As such, employees are required to respect the legal protection provided by copyright laws for computer programs, data compilations and for all other works (literary, dramatic, artistic or musical).

TFN employees are required to obtain proper permission for all programs, images or data stored, used and displayed on TFN systems.

Employees must also respect the legal protection provided by trademark law and the common law for names, marks, logos, and other representations that serve to distinguish the goods or services of one person from another.

2.3.1 Use and Copying of TFN Software

Software, licenses, product keys and usage rights to software used by TFN staff are the exclusive property of TFN. Any duplication of software or unauthorized use of any software (including such usage as specified or prohibited by the manufacturer or publisher of software), product key or license is strictly prohibited.

2.4 Intellectual Property Rights of TFN

All plans, reports and documents prepared by staff or consultants for TFN are the intellectual property of TFN.

2.4.1 Proprietary Rights and Monitoring

Intellectual property created by the employees and contractors of TFN in the course of their duties belongs to TFN and cannot be disclosed to third parties unless otherwise agreed to by contractual agreement.

Intellectual property, including email and Internet activity conducted using TFN property, is therefore subject to review and monitoring by others in TFN at any time. The authority to monitor and enforce this provision is held by the TFN Office Manager.

2.4.2 Disclosure of Intellectual Property

TFN intellectual property may be disclosed only on the consent of the C.A.O. or Council.

2.4.3 Improper Use of Intellectual Property

Improperly divulging or using intellectual property may lead to corrective action up to and including dismissal.

2.5 Virus Prevention

TFN employees are expected to take all necessary precautions to protect TFN information and technology systems from unauthorized use and from attack by worms and viruses.

It is forbidden to disable, corrupt, or otherwise render inoperable any portion of the anti-virus software installed on TFN computers and systems.

External storage devices must be scanned by TFN-managed virus scanning software before information contained on them may be used on a computer connected to the TFN's network.

2.6 System Access

TFN employees must not share the passwords to any accounts to which they have access and should take all necessary precautions to ensure that TFN IT systems and resources are not exposed to external bodies.

3. Information and Technology Management

Information and technology are valuable assets of the TFN used to support the outcomes of programs and services, as well as operational needs and accountabilities. The objective of this policy is to ensure that these resources are properly managed and maintained so as to retain their integrity and accessibility into the future.

3.1 Administration Access

Administrative access to TFN information and technology systems and resources shall be limited to TFN IT personnel and those granted written access by the C.A.O. This includes administrator passwords to access servers, network devices, and computers.

3.2 Rights over TFN Information

Data or information stored, used, or acquired in the course of performing TFN business is the exclusive property of TFN.

In addition, any communications in which TFN's information and technology systems are used (including correspondence such as e-mail) constitute TFN property.

Any other use, copying, or distribution of such information, including re-transmission of verbal information by any means outside of TFN, without prior approval from the relevant Department Manager or C.A.O. is strictly prohibited and may result in disciplinary action up to and including termination of employment.

3.3 Installation of Software and Hardware

Information software and hardware may not be added to the TFN network without the express written permission of the IT Department.

Installation of unlicensed and unapproved software on organization-owned computers is not permitted. This includes more recent versions of approved software.

4. System Audits and Monitoring

TFN reserves the right to control information technology resources.

TFN may conduct random software audits. Pirated, unauthorized or unlicensed software found during these audits may be removed or deleted when discovered without prior notice.

TFN may also, at its discretion, monitor and record or otherwise verify the contents of any network information ("traffic") by use of on-line monitoring, filtering, recording or scanning tools to identify inappropriate, excessive or unauthorized usage. Any material perceived to be harmful, unlawful, abusive or objectionable may be removed or deleted.

Violation of IT system and software usage policies may result in disciplinary action, up to and including termination of employment.