CITY OF NANAIMO

HUMAN RESOURCES POLICIES

Policy:	Acceptable Use of Technology	**Number:** 4.14
Applies To:	All Users of the City's Computer and Network Services	
Authorized by: Tracy Samra		**Effective Date:** November 1, 2017

PURPOSE

The City of Nanaimo makes available to its *Users* access to various forms of technology tools and services, including computers, laptops, software programs, e-mail, telephone and the Internet.

This policy outlines the City's requirements regarding the use of these *Computer and Network Services* and sets clear parameters for Users to ensure clarity surrounding the use of this corporate resource.

POLICY STATEMENT

The City provides Users with access to Computer and Network Services, including Internet use and email, to be used for legitimate business purposes in serving the interests of the City. These technologies are valuable tools that enable Users to effectively carry out the City's business.

Prior to the use of the City's Computer and Network Services, all Users are required to read this policy, including Schedule A (Use of Technology Standards) and acknowledge their agreement to comply with it.

Use of Computer and Network Services must be consistent with the City's Code of Conduct and Respectful Workplace policies. Users are expected to practice good judgment and to demonstrate responsibility and consideration of others when using the City's Computer and Network Services. All work undertaken shall be performed in an ethical and lawful manner, demonstrating integrity and professionalism by all Users.

CITY OWNERSHIP AND MONITORING:

1. All files and electronic communications, including email, Internet and web content systems, created on, generated by or transmitted through the City's Computer and Network Services are the property of the City of Nanaimo and subject to the *Freedom of Information and Protection of Privacy Act* (the "*FOIPPA*").

   Users should be aware that they have no right of ownership or expectation of privacy with regard to their use of the City's Computer and Network Services. If Users require a private means of computing and sending communications, they must use a personal device that is not connected to the City's Computer and Network Services.

2. All Users should be aware that the City's Computer and Network Services create activity records, including logs of every Internet site visited, every message sent through the City's corporate email system, every corporate electronic file accessed and every phone call made.

3. While the City of Nanaimo respects the privacy of Users, it still reserves the right to monitor use of its Computer and Network Services, including emails, where it has cause to suspect that the use of Computer and Network Services is not in compliance with this policy or other City policies and for the purpose of protecting and maintaining security. The City reserves the right to take action for these purposes, including accessing any files, information and equipment, as per the procedure detailed in the Auditing and Compliance section of this policy.

   Collection of personal information from the above monitoring activities is authorized under section 26(c) of the *Freedom of Information and Protection of Privacy Act ("FIPPA")*. Questions concerning the collection of personal information under these monitoring activities may be directed to the Director of Human Resources, 455 Wallace Street, Nanaimo, British Columbia V9R 5J6, (250) 755-4427 or to the City's Freedom of Information (FOI) Head, 455 Wallace Street, Nanaimo, British Columbia V9R 5J6, (250) 755-4494.

AUDITING AND COMPLIANCE

1. Where there are reasonable grounds to suspect misconduct or that a User has contravened this policy or another City policy, an audit of the User's usage may be undertaken with or without notice to the User under s.27 of *FIPPA*. Details of the investigation, including any evidence, shall be held in strict confidence and shall only be shared on a limited need-to-know basis.

2. Usage audits of Users may be requested by a manager to the Director of Human Resources ("Director"), or designate. The Director of Human Resources will confer with the Chief Administrative Officer and the FOI Head, or their designates, regarding the request. Upon approval, the Director will request the Information Technology Manager, or designate, to conduct the audit and report the findings back to the Director.

3. Usage audits of any User may be requested by law enforcement officials. In the event of such a request, records required for the audit will be collected by the Information Technology Manager, or designate, and provided to law enforcement as required by law or otherwise authorized by legislation.

4. The City retains the right to report any illegal violations to the appropriate authorities.

5. Failure to comply with this policy may result in the User's access privileges being limited or revoked and City employees may also be subject to disciplinary measures up to and including dismissal.

RESPONSIBILITIES

All Users

- Review this policy and request clarification from the applicable Manager if required.
- Ensure use of the City's Computer and Network Services conforms to this policy and to any other applicable legislation.
- Obtain authorization from management if an exception to this policy must be granted.
- Report any suspected violations of this policy to management.

Managers

- Ensure that their staff, hired contractors and other authorized *Users* comply with the provisions of this policy.
- Ensure that any policy exception request for supervised employees follows the procedure outlined in this policy.
- Report any suspected violations of this policy to Human Resources.

Human Resources ("HR") Department

- Promote awareness and understanding of this policy.
- Provide guidance to employees and Managers on the interpretation of this policy.
- Assist Managers and the Information Technology Department with investigations into contraventions of this policy, and advise Managers on the appropriate action to take when dealing with breaches of this policy.

Information Technology Department

- Perform appropriate monitoring of Computer and Network Services as outlined in this policy.
- Conduct auditing when suspected violations are reported by HR or another party.
- Assist HR in keeping this policy up to date by reviewing and recommending changes to this policy as required.

DEFINITIONS

- *Users:* means any individual who accesses or uses the City's Computer and Network Services, including but not limited to employees, contractors and members of Council.

- *Computer and Network Services*: means
  i. electronic hardware and equipment owned by the City including desktop, laptop, tablet, server or telephones (including analog, IP, and cellular), scanners, printers and fax machines and other peripheral devices and removable media (such as USB memory sticks, CDs, etc);
  ii. computer software, accounts and services owned, leased or subscribed to by the City, such as email, network file services, records management systems, SAP, Tempest, and any City-managed social media accounts or cloud services; and
  iii. transmission methods and services employed by the City, including wired, wireless and cellular networks, whether accessed from within the City's premises or elsewhere.

- *Non-public Information:* means information that is confidential or is exempt or is potentially exempt from disclosure under the *Freedom of Information and Protection of Privacy Act* ("FOIPPA").

RELATED DOCUMENTS

- BC Human Rights Code
- Canadian Charter of Rights and Freedoms
- *Freedom of Information and Protection of Privacy Act*
- Human Resources Policy 4.01 – Code of Conduct
- Human Resources Policy 4.09 – Respectful Workplace
- Information Technology Policy – Client Email List Usage Policy
- Information Technology Policy – Employee Owned Smartphone

- Information Technology Policy – Mobile Smartphone

PAST REVISIONS

- March 2016 - New policy created that consolidated the following:

Policy 4.14	Use of Computers and Electronic Communications
Policy 4.17	Personal Media Devices
IT Policy	Social Networking Policy

SCHEDULE A

Use of Technology Standards

USER ACCOUNTABILITIES

1. User Accounts

   User accounts and access to the City's Computer and Network Services shall only be provided to the degree required for Users to perform their authorized duties.

   Users are accountable for all activity conducted under their City accounts (e.g. network, e-mail, voice mail, online services or applications).

   - Users are responsible to protect these accounts from access by anyone other than themselves.
   - Generic user accounts must be authorized by the Information Technology Department.
   - Passwords for generic user accounts must not be shared with people who are not authorized to use these accounts.

2. Personal Use of City's Computer and Network Services and User-owned devices in the workplace.

   Limited, occasional or incidental personal use of the Computer and Network Services or User-owned devices in the workplace is acceptable, subject to the following conditions:

   - During working hours and non-core business hours, usage is brief and its volume, frequency or both does not disrupt City business, disrupt other Users or interfere with any employee work duties and responsibilities.
   - Usage does not bring the image of the City into disrepute or give rise to embarrassment or liability on the part of the City.
   - Usage does not put at risk the safety of any User.
   - Usage does not compromise the security or integrity of the Computer and Network Services or other City services, assets or information.
   - Usage complies with this policy, with all other City policies and with all relevant legislation, including FOIPPA.

   Specifically, the City's Computer and Network Services shall not be used for non-City purposes such as:

   - Selling merchandise, providing non-City services, running a personal business or any activity that could result in personal gain, with the exception of authorized electronic forums (such as classified ads) provided by the City for employee use.
   - Managing a personal website, accessing personal social media accounts or using personal email.
   - Storing large files or large quantities of files not related to City business on the City network.
   - Using their City e-mail address for non-work related subscriptions.
   - Performing work for profit with City resources in a manner not explicitly authorized by the City.

3. Conduct

The City's Computer and Network Services shall be used in a manner that is ethical, professional and compliant with the City's Code of Conduct, Respectful Workplace and other policies.

Such conduct demonstrates respect for intellectual property, City ownership of information, network and information technology asset security, and the rights of other Users to freedom from intimidation, harassment, and unwarranted annoyance. This policy does not answer every question or have rules for every eventuality; rather, it is designed to promote ethical decision-making and behaviour.

In particular, the City's Computer and Network Services shall not be used:

- For illegal or unethical activities, activities that do not meet community standards, or to support or assist such activities. This would include creating, posting, sending, downloading, or accessing discriminatory, violent, threatening, intimidating, harassing, or pornographic materials.
- To disrupt other Users or Computer and Network Services. Disruptions include distribution of unsolicited advertising, intentional propagation of malicious code (e.g., computer viruses or worms), sustained high volume network traffic (e.g., streaming audio or video).
- To download copyright protected material or other items where download is prohibited under the copyright holder's terms of use.
- To intercept network traffic unless engaged in authorized network administrative duties. The fraudulent interception of any computer or network function is an offence under the Criminal Code.
- To access Non-public Information which is not required for the User's duties.
- To circumvent or subvert network or system security measures (e.g. the disabling of anti-virus or patch management software).
- To send commercial messages without recipient consent.

4. Respecting Copyright

Using, copying, storing or transmitting copyright protected materials without permission of the copyright holder is prohibited. Users who do so shall be held personally responsible and liable for any activities resulting in copyright infringement.

5. Reporting Compromises and Breaches

A User who believes a breach of this policy has occurred shall immediately notify their Manager of the suspected breach. The Manager must report this breach to Human Resources ("HR") as per the procedure detailed in the Auditing and Compliance section.

INFORMATION SECURITY

1. Protecting Confidential Information

   Users shall ensure confidential information in their custody is protected from illegal, unauthorized or inadvertent use and disclosure, and shall observe access and privacy provisions of the *FOIPPA*.

2. Password Security

   For the protection of Users and the City, account passwords for network access, voice mail systems, and so forth, shall not be shared. Users must use their own City login credentials or approved generic account credentials to log into the City's Computer and Network Services. City-owned or User-owned cell phones and tablets which connect to the City's Computer and Network Services or store City information must be password protected. Passwords used to access City devices or information must follow current Information Technology Department password requirements.

3. Unattended Workstations

   Users shall not leave their workstation, laptop, or other device that is logged into the City network unattended without either locking it (Ctrl+Alt+Del Enter or WinKey+L) or shutting it down. Users shall not attempt to circumvent automatic unattended workstation locking mechanisms.

4. Shared Workstations

   Users shall logout of the network after each session when using a shared workstation to prevent unauthorized use of their network account, e-mail address and/or Internet access. Shared workstations that have been authorized for use with generic accounts must be treated in accordance with the "Unattended Workstations" section.

5. Data Storage and Recovery

   City information shall be stored on either a corporate database or service, on a corporate shared network drive or on a corporate personal network drive. Other storage media should only be used to store, with appropriate security controls, copies of City Information, as information on these storage mediums will not be backed up by Information Technology Department and cannot be restored should the storage medium be damaged.

   Non-public information may not be stored on portable devices without applying industry-standard encryption mechanisms to prevent disclosure in case of loss or theft.

   City of Nanaimo information may not be stored on or transferred to servers located outside Canada. This includes transfer of City information to personal email or cloud storage facilities, such as Gmail or iCloud. Storage on external Cloud-based services requires written authorization from Information Technology Department management. This restriction does not apply to City-provided cloud storage (e.g. cloud.nanaimo.ca).

HARDWARE AND SOFTWARE SECURITY

1. City Property Identifiers

   Identifiers affixed to City Property equipment shall not be removed.

2. Damaged or Lost City Property

   Users are required to report any damage to or loss of City property covered by this policy to the Information Technology Department immediately. The City is not responsible for any misuse of Computer and Network Services. Persons found to be misusing the City's resources will be held accountable, and will be required to indemnify the City for any claims against the City.

3. Safeguarding Information Technology (IT) Assets

   Users are required to protect the availability of Computer and Network Services by guarding against accidental damage, theft, loss and environmental hazards. City assets, including mobile devices such as laptop computers, tablets, smartphones, shall be safeguarded from public access using approved physical and logical security controls as authorized by the Information Technology Department.

   City devices that support remote data destruction must have this functionality enabled. If technology allows, a remote wipe of all data, both personal and business, must be performed if a device storing City of Nanaimo information is lost or stolen.

4. City Hardware

   Prior to purchase, hardware intended for connection directly or indirectly to the City's Computer and Network Services must be authorized by the Information Technology Department to ensure that it does not pose a security, compatibility, or network stability threat.

   Network devices, such as access points, routers, switches and hubs must not be connected to the City's Computer and Network Services without first obtaining the written approval of Information Technology Department management.

5. Non-City Hardware

   Non-City computing devices such as smartphones, tablets, laptops and other networked devices, are not to be directly connected to the City's *Computer and Network Services* without the written authorization of the Information Technology Department.

6. Software Installation

   Users may not purchase, develop, download, or attempt to install software without first obtaining authorization from the Information Technology Department to ensure security and compatibility with Computer and Network Services and that sufficient resources are in place to support the software. All software must be properly licensed and used only in accordance with its respective Software License Agreement.

COMMUNICATIONS SECURITY

1. Internet Use

   The Internet is an open, non-secure information network. Users shall not visit Internet web sites such as those:
   - which are inappropriate for business functions of the City or do not support the operating principles and practices of the City;
   - with a strong potential to cause a network security breach.

   Websites representing a security risk to the Computer and Network Services will be automatically blocked where possible, but Users should always be cautious and aware that security risks may develop faster than blocking technology can be updated.

2. Electronic Mail and Messaging Services

   Users shall conduct email messaging in the same manner as they would other business correspondence, being mindful of the fact that email transmissions over the Internet are not secure and may be intercepted.

   City business emails must be sent and received through the corporate email system. Users should not send business-related emails to or from a personal email account. Users must not conduct City business via text messages.

   Users shall be vigilant when using the e-mail system. Suspicious e-mails, in particular the attachments, shall not be opened as they may contain malicious code (e.g., viruses, worms, trojan horses, etc.). Suspicious e-mails must not be responded to and should be deleted immediately.

3. Remote Access to City Network

   Users shall remotely access the City's Computer and Network Services only by methods authorized in advance by the Information Technology Department, such as Citrix, Virtual Private Network (VPN), ActiveSync and Mobile Device Management software.

   Any City-owned or User-owned devices used to remotely access the Computer and Network Services shall meet the current Information Technology Department requirements for device configuration, such as current operating system updates and, for Windows devices, presence of a current and updated anti-virus program.

   Devices shall not be connected both to a public Wi-Fi network and a City physical network port at the same time. This configuration potentially allows remote access to the City network, bypassing critical network security layers.

4. Social Media

   The City uses social media to better inform and engage Nanaimo residents and stakeholders; therefore, the City's social media accounts should be used only for official City communications.

All communications on social media should contain appropriate and respectful language. The following guidelines provide Users with parameters for conversation:

- Be thoughtful about how you present yourself in online social networks.
- Protect the City of Nanaimo's confidential and proprietary information.
- Respect your audience, your coworkers and members of Council.
- Add value.
- Use approved City messages.

The City will ensure that its engagement of the public on social media platforms is conducted in a manner that does not harm the reputation of the City or lead to potential liability on the part of the City. This will include restricting or removing any individuals or comments that are disrespectful towards staff, elected officials or other citizens. Designated members of senior management may monitor all City social media accounts in furtherance of this objective.

Users should take into consideration that all information produced using the Computer and Network Services is City property and considered public knowledge. Users have no expectation of privacy when using the Computer and Network Services.