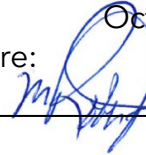


Acceptable Use of Information Technology

Effective Date: September 4, 2012

Last Revised: October 24, 2024

CAO Signature:



1. Purpose

To establish a set of rules that define the ways in which City Information Technology should be used at the City.

2. Scope

This policy applies to the use of all City Information Technology owned, leased or licensed by the City of Pitt Meadows and applies regardless of physical location.

3. Exclusions

The Chief Administrative Officer may grant standing or single instance exemptions to this policy where a valid business reason exists.

4. Definitions

In this policy,

- (a) **Personal Computing Device** means any computer device or peripheral used by an individual including but not limited to a desktop computer, laptop, smartphone, handheld, tablet, mouse, keyboard, monitor, storage or network device.
- (b) **Mobile Client Computing Technology** includes all cell phones, smartphones, laptop computers, tablet computers, mobile internet sticks, mobile device usage plans and related peripherals.
- (c) **Social Media** means any form of online presence or publications including but not limited to YouTube, Facebook, X, Instagram, blogs, wiki, etc. that provide a platform to engage in social networking activities or publish

content on the internet. Social messaging applications including chat, SMS, MMS and related applications are also included under this definition.

- (d) **Generative Artificial Intelligence (AI)** is a type of artificial intelligence technology that can produce various types of content, including text, imagery, audio and synthetic data.

5. Policy Statements

The City of Pitt Meadows provides computers, email, mobile devices, print, facsimiles (fax capability), data network, internet access, software and other technology (herein referred to as “City Information Technology”) to elected officials, employees, volunteers, contractors and other persons (herein referred to as ‘Users’) for conducting City business. Anyone using City Information Technology must comply with all applicable federal and provincial laws, the specific conditions set out in this Policy and all other City policies as they apply.

5.1. Roles and Responsibilities

N/A

5.2. Prohibitions

N/A

5.3. Guidelines and Procedures

City Information Technology is provided to Users primarily for conducting business on behalf of the City. Limited personal use of City Information Technology is permitted on the conditions listed below under “Acceptable Use”.

All information sent, received or stored using City Information Technology is within the custody of the City and is therefore considered City information. This includes but is not limited to documents, correspondence, e-mails, database records and internet browsing records. The *Freedom of Information and Protection of Privacy Act* (the Act) applies to all City information and could be subject to release under the Act. The City will comply with all reasonable requests from law enforcement, regulatory agencies and FOI requests for information that is accessible under the Act.

Additionally, in some circumstances, the City has the right, but not the obligation to monitor the use of City Information Technology and may do so at any time.

Individuals who wish to engage in personal use of City Information Technology with an expectation of privacy should instead use a personal computing device.

Acceptable Use

- City Information Technology is provided for users primarily to conduct business on behalf of the City. This includes but is not limited to the production of correspondence and reports, e-mail communications, social media communications and Internet use.
- Personal use of City Mobile Devices is allowed provided it does not interfere with City business and does not place the City or its property, staff, reputation, or data at risk.

Unacceptable Use

It is a violation of this policy to use City Information Technology in the following ways:

- Access City Information Technology, information or accounts without proper authorization.
- Grant another individual access to one's own information technology accounts by sharing credentials of any kind (including user ids and passwords) unless sanctioned by City IT for legitimate purposes.
- Access, create, publish, store or communicate information with the following content:
 - Gambling
 - Pirated, hacked, or unlicensed content
 - Pornographic or adult content
 - Illegal activities
 - Other content that could be deemed racist, defamatory, discriminatory or hateful
- Entertainment software, games, or playing games against opponents over the internet is not permitted on City laptop or desktop computers. Use of this software is permitted on City iPhones if done on the users own personal time and doing so does not interfere with City business.
- Upload any software licensed to the City or data owned or licensed by the City without proper authorization from the IT Manager.
- Replicate or transfer City information outside of the City's network unless explicitly permitted by the City Clerk or their delegate.



- Use City Information Technology in any way that intentionally interferes with the normal operation of the City, its partners or stakeholders.
- Circumvent or attempt to bypass the security measures put in place by City IT.
- Use City Information Technology for personal gain or profit.
- Defame, libel, threaten, harass, or offend others, including under the guise of 'course of business'.
- Transmit copyrighted, confidential or protected information to unauthorized users or the public.
- Gain unauthorized access to copyrighted, confidential or protected information.
- Any activity that could be seen as a violation of the Criminal Code.
- Deliberately propagate malicious content including virus, malware, ransomware or anything that could harm another electronic device.
- Defame or compromise the integrity of the City or its employees.
- Send unsolicited messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
- Initiate any form of harassment.
- Impersonate other individuals or organizations.
- Solicit individuals or organizations with the intent to harass or obtain unauthorized information.
- Create or forward "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Internet Use

Internet use must comply with the rules of use of City Information Technology as defined in this policy.

City IT may block access to certain websites and services based on specific categories or risk to the City. If access to a website or service is blocked, users may submit a request to IT Support for authorization to access such pages. Users must not try to bypass such restrictions on their own.

The City maintains a record of internet activities. The City may be required by law via the *Freedom of Information and Protection of Privacy Act* to submit these records to the public.

Email & Communications

The use of email and other City communications technology must comply with the rules of use of City Information Technology as defined in this policy.

As noted above, the City maintains a record of internet and email activities and may be required by law to submit these records to the public.

Personal Use of Social Media

Limited or occasional use of City Information Technology to engage in social media for personal use is acceptable as long as:

- It is done in a professional and responsible manner.
- Does not violate this or other City policies.
- Does not interfere with an employee's regular work duties.
- Users do not publish any City information on social media or internet websites that is confidential or has not been approved for public disclosure.
- Users do not give the impression that comments, opinions, or statements made on social media or internet websites represent the views of the City without prior approval.
- Users do not publish comments, opinions or statements that are likely to negatively affect the City's reputation or are contrary to the City's core values.
- Users do not engage in any form of social media that may harm or tarnish the image, reputation and/or goodwill of the City, its employees or constituents.
- Users do not attribute personal statements, opinions or beliefs to the City when engaging in social media. If a User is expressing his or her beliefs and/or opinions in blogs, the User may not, expressly or implicitly, represent themselves as an employee or representative of the City.
- Users assume all risk associated with the personal use of social media.

Use of External Storage Devices and Other Peripherals

City IT issued external storage devices such as memory sticks (thumb drives) and other removable hard drives can be used only in situations when network

connectivity is unavailable or there is no other secure method of transferring data from one device to another.

Users should not connect any personal computing device, storage device or peripheral to City Information Technology unless explicitly approved by IT. This includes but is not limited to monitors, mice, keyboards, laptops, network devices, printers, thumb drives and other external storage devices. Personal smartphone's may connect to the City's guest Wi-Fi network.

Externally Hosted IT Services

Users should not use any externally hosted IT services for the purpose of storing or sharing City information unless explicitly permitted by IT and permissible under FOIPPA. This includes the storing or sharing of City owned information that is personal or confidential in nature using services that are not owned, managed and controlled by the City. These services include but are not limited to cloud computing platforms and software services, social networking applications (i.e. all social media, blogs, and wikis), file storage & sharing services (e.g. Dropbox), external email services (e.g. Gmail), content hosting services and cloud syncing and back-up services for mobile devices (e.g. iCloud, Evernote, OneNote).

Exceptions must go through both the City Clerk's Office and the IT Department. Users who are unsure what constitutes confidential information should check with the City Clerk's Office.

Mobile Communications Devices

This policy extends in its entirety to City Mobile Devices. Policy A002 (Mobile Client Computing Technology) defines the specific terms under which City Mobile Devices may be issued to and used by City staff.

Use of Generative AI

Users are permitted to use Generative AI platforms including ChatGPT and other internet based conversational chatbots for general informational purposes. When using these technologies, users should use information that is publicly available and should always verify the accuracy of generated content. The following are ways in which generative AI platforms should not be used at the City:



- Do not use with any public body record that contains personal, sensitive or confidential information. For example, do not include names, addresses, or any personal identifiers in the chatbot. Do not include any quasi-identifiers that could identify people if combined with other information that the chatbot has access to.
- AI platforms may produce or consume inaccurate or biased information and therefore should not be used as a sole factor in decision-making. AI may be used as a research tool and to assist in decision-making, however users should always strive to verify the quality and accuracy of information generated from AI platforms prior to using that information in decision-making.
- Do not use to replace human expertise or judgement.
- Do not post information that you would not post on a public site or social media.

6. Related Policies

Other related policies include:

- (a) A002 Mobile Client Computing Technology
- (b) A052 Software Asset Management Policy