Township of Langley

HUMAN RESOURCES POLICY

ACCEPTABLE USE OF TECHNOLOGY

(previously Electronic Mail, Internet Use and Virus Protection, Computer and Communications Systems)

APPROVED:	DECEMBER 12, 2000	REVISED:	JULY 13, 2004 FEBRUARY 21, 2008 JULY 22, 2008 JANUARY 15, 2010 JULY 27, 2010 DECEMBER 9, 2010 MAY 5, 2011 NOVEMBER 21, 2011 AUGUST 4, 2015

PURPOSE

The intent of this policy is to outline the parameters for the acceptable use of technology. This policy applies to:

- data transmitted or stored via information systems
- the usage and protection of physical assets
- employees and individuals completing work on behalf of the Township of Langley

BACKGROUND

The Township of Langley supports the principle that technology is integral to daily operations. Employees are provided with access to various information systems and devices as tools to perform daily work.

Employees or individuals working on behalf of the Township are placed in positions where integrity, honesty, and trust are essential elements and are expected to conduct themselves in an exemplary and trustworthy manner.

POLICY

General

Under no circumstances is an employee or individual working on behalf of the Township of Langley authorized to engage in any activity that is illegal under local, provincial, federal, or international law while utilizing Township information systems or devices. It is imperative employees understand the Township of Langley is implicitly represented in all instances in which the organization's computer systems are being used. Employees shall maintain a professional, business presentation in the use of these systems in accordance with the Township's Communications Protocol.

Communications, including personal messages stored on the Township's information systems, are records belonging to the Township of Langley and are subject to the Freedom of Information and Protection of Privacy Act. The Township may, at the discretion of management, access and review at any time any record stored in its systems. An employee or non-employee associated with the Township must not assume they have privacy with respect to the contents of any documents that utilize Township information systems or devices.

To ensure the integrity of the Township's information systems, related equipment, and the Township itself, several activities are neither appropriate nor permitted when using the Township's information systems or devices. These activities include but are not limited to:

- duplicating, storing, or transmitting obscene, sexually explicit, or pornographic materials
- using vulgar, profane, or inappropriate language
- sending defamatory, derogatory, or false messages
- transmitting or posting threatening, abusive, or obscene material
- inappropriate disclosure of Township documentation or information
- engaging in for any purpose anything illegal or contrary to Township of Langley policy or business interests

If employees are unsure an activity would be considered inappropriate, they should refrain from participating in the activity and follow up with their supervisor/manager.

Employees must respect the confidentiality of other individuals' electronic communications. Except in cases where explicit authorization has been granted by Township management, employees are prohibited from engaging in or attempting to engage in:

- monitoring or intercepting files or electronic communications of other employees or third parties
- hacking or obtaining access to systems or accounts they are not authorized to use
- using other's log-ins or passwords
- breaching, testing, or monitoring computer or network security measures
- circumventing user authentication or security of any host, network, or account

- revealing account passwords to others or allowing the use of your account by others. This includes family and household members when work is being done at home.

Employees found to be engaged in the inappropriate use of information systems or devices, including but not limited to electronic mail or the internet, may be subject to discipline up to and including termination of employment from the Township.

Device Resources and Usage

Portable devices are entrusted to the user, who is fully accountable for their use and security. Loss of the device, or unauthorized access, exposes the Township to risk related to the security of its systems as well as loss of the physical asset. Loss of a Township information technology device or a device configured to access a Township information system must be reported to the Township's Information Technology Department Helpdesk immediately.

Employees are prohibited from acquiring and/or installing **any** technology product or service (e.g. computers, software, hosted solutions, telephony, etc.) without prior consent from the Information Technology Department.

Information systems or devices cannot be used in a manner that could cause network congestion or significantly hamper the ability of others to access and use information systems. The use of high bandwidth activities, such as streaming audio and video, is restricted unless pertaining specifically to Township-related work activities.

Employees must power off their devices at the end of the workday unless otherwise approved by the Information Technology Department. In addition, for security reasons, employees must lock or log off their computer when expected to be away from their work area.

To ensure the Township's systems are secure and meet operational needs, employees cannot connect any device (e.g. USB, iPod, smart phone, etc.), regardless of ownership, to a Township system without expressed authorization from their director/general manager and the Information Technology Department.

Employees authorized to conduct Township business remotely are not permitted to store Township information on non-Township systems or devices. Employees working remotely must contact the Information Technology Department to ensure the appropriate protocols and data storage are used to ensure the integrity and security of the information generated.

Any device connecting to a Township system must have up-to-date malware detection software, all required security patches installed for known vulnerabilities, and a password applied to secure the device from unauthorized use.

Passwords applied to protect information systems or devices must conform to the information technology System Password Standard.

Personal Use

Employees may, upon approval from their director/general manager, be permitted to use electronic mail and/or access the internet for personal purposes providing such use does not interfere with the day-to-day operations of the Township and that such use is acceptable as defined in this policy.

Personal use must, to the greatest extent possible, be confined to break times and off duty times. Personal use of the Township's computer and communications system are not private and are subject to Township access, control, and monitoring.

When employees use their own personal computer, a public computer, or another private computer to access personal blogs or personal social media sites, employees can be subject to discipline for inappropriate comments relating to their employment and/or the Township; including, but not limited to, areas such as:

- insubordination
- defaming customers, fellow employees, managers
- prohibited ground of harassment
- breach of confidentiality
- other prohibited disclosures

The Township may monitor employee's personal and public sites and will investigate all incidents of inappropriate activities or misconduct.

Employees found to be engaged in the inappropriate use of information systems or devices, including but not limited to electronic mail or the internet, may be subject to discipline up to and including termination of employment from the Township.

RELATED POLICIES AND REFERENCES

Code of Ethics, Confidentiality, and Conflict of Interest Policy; Communications Protocol; Respectful Environment Guidelines; Respectful Workplace Policy; Freedom of Information and Protection of Privacy Act; Media Policy; Corporate Identity Manual; Customer Service Standards; System Password Standard; and generally accepted records management principles.