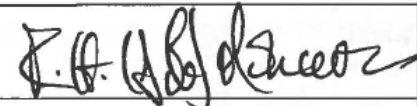
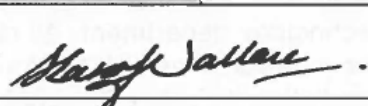


**Acceptable Use of the City of Burnaby's Email Systems
Statement of Policy and Procedure**

Department:	City Manager's Office	Division:	Information Technology
Policy area:	User Responsibilities		
Policy No.:	IT 13.0A		
Subject:	Acceptable Use of the City of Burnaby's Email Systems		
Issued to:	All City staff		
Issued date:	2015 September 30	Effective date:	2015 October 23
Approved by:			
	City Manager – Bob Moncur	Chief Information Officer – Shari Wallace	

1 PURPOSE

Helping to maintain the online reputation of the City of Burnaby and City staff is important and a key focus of Information Technology. The purpose of this policy is to ensure that all staff are informed of how to present themselves and represent the City in a professional manner when using email and that appropriate measures are taken to:

- (a) Prevent the unauthorized or inadvertent disclosure of sensitive information
- (b) Protect the City's information technology assets from viruses and malware that use email as an entry point to an otherwise secure organization

2 SCOPE

This policy covers appropriate use of any computing device using City of Burnaby resources for storing, transmitting or processing email, and applies to all employees, vendors, and agents operating on behalf of the City, whether on site or working remotely.

While this policy does not address email retention, staff should be aware that emails may be subject to the British Columbia *Freedom of Information and Protection of Privacy Act* ("FIPPA"). Additional information is found on the portal in References & Support, under Records and Information Management, and on the BC Ministry of Technology, Innovation and Citizens' Services website for Records Management.

3 POLICY

- 3.01 Staff using City supplied equipment and network resources for conducting City business should assume that their email communications are not private. All email received or sent through City-owned systems and networks are subject to logging, archiving and inspection for the purpose of investigating and documenting violations of City policies.

Limited personal use of City email accounts and software is acceptable provided it does not affect job performance, is not for personal financial/commercial or third party gain and that the user adheres strictly to this policy. While content of personal email accounts (e.g., Gmail, Hotmail, Telus, etc.) are considered private, the use of City resources to retrieve and send personal email are still subject to IT 13.0 Acceptable Use of City of Burnaby's Computing Technology and Network Resources policy.

- 3.02 All users of City-provided email are prohibited from sending email that:
- (a) Is offensive, defined here as any image or graphic that is defamatory or libelous, harassing, menacing, threatening, obscene, pornographic or sexual in nature, containing otherwise offensive language or content, or has other malicious intent
 - (b) May damage employee morale or cohesiveness such as jokes, gossip, rumours, innuendoes or disparaging remarks
 - (c) May be construed as spam or chain letter emails
 - (d) Knowingly or negligently includes malware, in the form of attachments or Internet links to viruses, Trojan horses, worms, spyware, and other forms intended to expose City systems and networks to malicious intent
 - (e) Is used to enable a personal business venture and not related to the City's business
 - (f) Tries to mask the identity of the sender or masquerades as having come from a different sender
 - (g) Violates information copyright
 - (h) Is received from another City account and automatically forwarded to an external destination (non-City account) without prior management approval

- 3.03 City email account holders should not back up email items onto personal or other non-City storage devices. All City email must remain stored on City owned equipment only.

- 3.04 IT Infrastructure monitors email usage on a regular basis as part of capacity and performance management of the City's email systems. Within this mandate, any incidental discovery of inappropriate use of the City's email systems and software will be brought to the attention of the employee's supervisor and the Human Resources department.

- 3.05 For employees, failure to comply with Information Technology acceptable use policies or other associated policies, standards, guidelines, and procedures

may result in remedial action appropriate to the situation and may range from warning to dismissal.

For contractors or consultants, failure to comply with Information Technology acceptable use policies or other associated policies, standards, guidelines, and procedures may result in remedial action appropriate to the situation and may range from warning to termination of contracts.

4 RESPONSIBILITY

- 4.01 All City email users who have access to the City's electronic and communications tools are responsible for understanding and adhering to this acceptable use policy for email systems.
- 4.02 The Director, Human Resources and the Chief Information Officer are responsible for interpreting this policy, as necessary, and for recommending revisions.

5 DEFINITIONS

- 5.01 **"Chain Email/Letter"** – email sent to successive people, typically with content in the body of the note that has direction to send out multiple copies of the note in return for good luck or money.
- 5.02 **"Sensitive Information"** – refers to information that is confidential such as personally identifiable information and credit card data, or of high value such as information pertaining to security of critical infrastructures. The disclosure of sensitive information may be a violation of the British Columbia *Freedom of Information and Protection of Privacy Act*, interrupt the City's ability to deliver services, lead to financial losses related to correcting the situation, legal actions, and erosion of public trust in the City.
- 5.03 **"Unauthorized Disclosure"** – intentional or unintentional revealing of sensitive information to individuals, either inside, outside of the City, or both, who do not have a legitimate need to know that information.
- 5.04 **"Spam"** - as applied to email means unsolicited bulk email. Unsolicited means that the recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantially identical content. A message is spam only if it is both unsolicited and bulk.

6 REFERENCES and RELATED STATEMENTS of POLICY and PROCEDURE

IT 13.0 – Acceptable Use of City of Burnaby's Computing Technology and Network Resources

IT 13.03 – IT Password Policy

Social Media Use Policy

Voice Mail Policy

Respectful Workplace Policy

FOIPPA Policy & Procedure Manual

British Columbia *Freedom of Information and Protection of Privacy Act* ("FIPPA")

7 PROCEDURES

- 7.01 Messages from unfamiliar sources must be immediately deleted and purged unless there is evidence that the message may be legitimate. Suspicious email must be thoroughly investigated by IT staff before it is opened to determine the source and objective of the email.

The City uses anti-virus software to filter out emails with attachments that have specific file types that may carry viruses, worms, Trojan horses, or other executable items that could pose a threat to the security of its systems and network. In addition, the City applies rules to incoming emails to reduce the number of unsolicited commercial email (i.e. spam).

Users should expect that there is always a minute chance that legitimate email items addressed to themselves may be subject to the City's Spam filters and therefore never arrive in their City mailbox. If a user suspects this is the case, IT Help Desk should be contacted to assist in their recovery.

- 7.02 Users are expected to limit email congestion by distributing email to the smallest group possible and refrain from sending or responding to chain email.
- (a) Email messages sent to all employees via *All Subscribers* are not permitted. Each department has designated staff who can send email messages to *All Subscribers*. Senders who have a requirement to message all staff should consult with their designated departmental representatives
 - (b) Rather than sending large attachments, users should use a reference or link to a document stored on the City's portal or Common File Server. (*Note: Files should be deleted from the Common File Server after the documents are no longer required*)
 - (c) Users should take care in directing messages to large audiences and avoid repeatedly re-sending messages as "reminders"
 - (d) Unless part of a corporate initiative, use of City email to promote non-profit campaigns should be limited to known acquaintances

- (e) Personal promotions (business related sales) or non-City business promotions or offerings using the City's email system are not permitted
- 7.03 Personal and corporate liability could result from offensive materials being stored on or distributed from City servers/PCs. Employees who receive any emails with this content from any City of Burnaby employee or contractor should report the matter to their supervisor immediately.
- 7.04 Users are not permitted to make financial/commercial/legal commitments on behalf of the City via a City email account without appropriate authorization as an email message is recognized by law as potentially binding like other written documents.
- 7.05 Sensitive data such as credit card, banking, or private personal information are not to be sent via email. If there is a critical need and time sensitivity to send such data, staff should contact the IT Helpdesk for secure transmission alternatives.
- 7.06 Employees and contractors are not permitted to use non-City email accounts (i.e. Hotmail, Yahoo, Gmail, Shaw, Telus, etc.), or other external resources to conduct City of Burnaby business, thereby ensuring that (1) official business is never confused with personal business, and that (2) City sensitive data does not find its way on to external email systems.
- 7.07 To avoid proliferating hoax or outdated notices of virus warnings, only designated IT staff may send out such notifications. If any staff receive warnings not sent by IT, the IT Helpdesk should be notified in order to assess the validity of the warning.
- 7.08 Employees are responsible for email sent from their accounts, underscoring the importance of not sharing City system and network credentials with anyone else.
- 7.09 Employees going on vacation should first set their "Out of Office Assistant" in Outlook. This avoids any need to send out messages about vacations. The "Out of Office Assistant" will send an email message to anyone who tries to contact a City employee while away on vacation. The message should contain a signature file. See 7.10.
- The message should state the day and month of return and include a person to contact if the issue is urgent. An "Extended Absence Greeting" should also be created in Voice Mail as per the Voice Mail Policy. At the end of the vacation, employees should remember to re-set their "Out of Office Assistant" and "Extended Absence Greeting" messages.
- 7.10 All emails sent through the City must contain the true identification of the sender. The forging of return addresses will not be tolerated. All employees are to set up an Outlook signature file (Outlook->Tools->Options->Mail Format) within their email account that denotes their name, job title, department, floor (if warranted), building address, email address, office phone & fax numbers.

The City's employees and/or consultants using the City's Outlook Signature File must also include the following disclaimer which must be setup to automatically be appended to all sent messages:

The contents of this posting or electronic mail message are solely the writings, thoughts and/or ideas of the account holder and may not necessarily reflect those of the City of Burnaby.

8 ATTACHMENTS

None