Township of Brock Corporate Policy

Policy Name: Email Etiquette Policy

Policy Type: Administrative

Policy Number:

Reference:

Date Approved:

Date Revised:

Approval By: (most cases Council)

Point of Contact: Manager IT

Policy Statement

The Corporation of the Township of Brock ('the Corporation') is committed to providing all persons with a level of conduct through all means of communications including electronic mail (email).

Purpose of the Policy

This policy provides guidelines for the proper use of electronic mail as a means of communication to ensure the safety and integrity of the Corporation. This policy applies to all users of the Corporation's email system.

Definitions

Email: Means messages sent through an electronic system to groups or individuals. This shall include components of calendars, notes, tasks and/or contact.

Inappropriate: Means an email containing offensive text, art, photos, cartoons or any graphic manner or harassing, menacing, threatening, obscene, pornographic or sexual in nature or having other malicious intent.

Malicious email: Means any email that would be classified as Phishing, Spear Phising or Spam and/or contains internet links to unsecured or malicious websites or contain malware attachments.

Phishing: An attempt to gain access to confidential information such as personal information, credit card information, banking information, usernames/passwords or other information to gain access for fraudulent purposes.

Spear Phishing: Means posing as a known person or contact in order to directly access usernames, passwords or similar information. This is usually directed towards one person or select persons as opposed to Phishing which is much more broad in nature.

Malware: Means software designed to infiltrate or damage computer or network systems. Common forms of malware are viruses, worms, Trojans, spyware, adware and ransomware.

Procedures

When conducting Corporation business by email, only the Corporation's Microsoft Office 365 mail system is to be used. Personal email accounts are not permitted to be used for Corporation business.

Users are permitted to use personal devices to access the Corporation's email through the secure O365 Microsoft app using the credentials provided by the Corporation.

Security

Users are required to delete and report all suspected malicious emails immediately. Suspected spam mail should be forwarded to techsupport@brock.ca for review.

If any user suspects their email account has been compromised, they are responsible to advise their Department Head, Manager of IT and Durham Region IT Help. This should be accomplished by phone or in person, where applicable.

Users are responsible for guarding the passwords of individual and shared mailboxes. Passwords are not to be shared with other staff or persons outside of the Corporation. All passwords must be shared with the Manager of IT.

Privacy

All emails sent or received through the Corporation email system are the property of the Corporation. Bulk deletion of emails is not permitted unless approved by the Department Head and may be subject to retention requirements.

All users should assume all email messages are not private and may be made public as part of an internal audit, judicial or other public disclosure (MFIPPA)

Email Etiquette

Make it Easy to Read and Respond to

- Put your most important information in the first paragraph and supporting information in the following one or two paragraphs
- Make the subject line concise, descriptive and informative so the subject is known before opening the email
- Write short, easy to read sentences and paragraphs

Formulate the Message

- Give an introduction
- Identify the question, issue, problem, opportunity
- Place the message in context

Time Manage E-Mail

- Set aside specific time to see what has arrived and what is important
- Don't interrupt yourself every time an email message arrives
- Make your response short. Give "Yes" and "No" answers when possible and if you have to write a few sentences or paragraphs, make them concise and to the point
- For email messages that are unrelated to your responsibilities, ask the sender to remove you from their list
- Misdirected messages should be returned to the sender and deleted

Figure Out the Audience

- Consider who you want to send the message to
- Think about the message you are preparing and how it may create a cascade effect after being sent
- Decide who the main recipient is and who should be copied
- Avoid using the reply all option and only respond to the sender when appropriate
- Avoid sending large attachments to large distribution groups. Make use of common shared drives or One Drive

Be Careful with the Freedom of Email

- All messages create an electronic record
- When writing internal email messages, use the same dictation, complete sentences and common sense as if you were writing a letter, have a conversation on the phone or a face to face meeting
- Create single subject messages to aid in file storage, retrieval and forwarding

Remember OADA requirements

- Use upper and lowercase letters in the same manner as if writing a letter
- Use bold for emphasis, not italics or underlining
- Use contrasting colours for background and foreground. Black text on white background is the best contrast and easiest to read

Signatures and Out of Office Messages

- All users will use a standardized email signature provided by the Corporation. The standardized signature may be customized for each individual staff member (i.e., name, telephone number, preferred pronouns) but should not otherwise be modified.
- Out of office messages should be enabled by all users whenever they are away from work for an extended duration (i.e., one day or more). Out of office messages should contain the following information:
    - Duration of absence
    - Alternate contact for urgent matters
    - Whether you will be checking and responding to email periodically or if you will be unresponsive for the full duration