

Email Use Policy

Purpose

The City of Milwaukee encourages its employees to use email for work-related communications, to assist in providing services to citizens, and for any other activity that supports the city's mission. The use of email, while convenient, does not come without expectations and risk to the City. In order to demonstrate these expectations and risks the following policy should be followed by all City employees.

Scope

This policy applies to all City-issued email accounts.

General Policy

Access

City departments will request email accounts from the Information and Technology Management Division (ITMD) when a new employee is hired. The appropriate email access will be granted by ITMD in consultation with the requesting manager.

ITMD will disable Email use as defined by the Email Account Termination policy.

City departments are encouraged not to request email accounts for contractors, vendors, or agents of the City. If contractors use a City email account they must identify themselves in the signature block as non-city employees and they must comply with all policies, rules, and requirements regarding use of the City's email system; including being subject to open records searches and no expectation of privacy. Any reference in this document to "employee" or "City employee" shall be considered to include any contractor, vendor, or agent working for or representing the City with a City email account.

Acceptable Use

City employees must use only the City's email to send and receive messages for work-related communication or for official communication with constituents. Employees may not use personal email accounts to conduct any type of official City business. Under no circumstances will employees be permitted to use city equipment and email systems for illegal activities, profit-making ventures or political endeavors.

Employees must also abide by all applicable laws, policies, and guidelines regarding the appropriate use of email. They may not send messages that can be construed as scandalous, defamatory, libelous, obscene, immoral or in violation of any intellectual property rights. Email users may not knowingly misrepresent themselves or their employment by the city; in messages sent they must always identify themselves honestly, accurately, and completely.

The City acknowledges that incidental use of the city's email system for personal purposes may be appropriate. However, departments must ensure that such use does not impair the employee's ability to fulfill his or her job responsibilities.

Privacy and Security

All email sent from or received are considered City property. City and departmental management reserve the right to examine, at any time and without prior notice, all email. Users should not assume any privacy or confidentiality for messages they transmit or receive via the City's email system. Users should never send confidential or sensitive information via unencrypted email.

Email passwords are to be kept safe and private. No employee should provide their password to another employee to access their account. If this is necessary due to extended leave or other business reasons, contact ITMD helpdesk or enter a RITS ticket to set up alternative means of access rather than sharing passwords.

Encrypted Email

It is not advised to send confidential or personal identifiable information via email. When it is necessary to send confidential or personal identifiable information via email to an address other than a milwaukee.gov account, please contact ITMD for instructions on how to send an encrypted email.

Encrypted emails sent to the City from outside sources are not searchable for the purposes of open records. Encrypted emails should only be received by the City when required by federal, state, or local law, and it is the responsibility of the City user to save these documents to a file system. The email body message and any attachments should be saved in an appropriate storage medium to ensure it is retained and searchable for the length of the record retention. Questions should be directed to ITMD, the City Attorney's office, or the City Records Manager in the Office of the City Clerk.

Archiving and Record Retention

The City's email archival system will automatically store all email messages sent or received through the City's email system. All emails contained in the archival system will be subject to public disclosure under open records laws.

Transferring Employees

Due to the increased volume of open records request for email, all employees transferring from one department to another will get a new email account. The change will result in the old mailbox staying with the original department. For example, a user in ITMD with an email of nrobles@milwaukee.gov moves to Comptroller's office. The account nrobles@milwaukee.gov is disabled and remains within ITMD. The employee will receive a new email of nrobles2@milwaukee.gov which is associated with the Comptroller's office. The account alias of Nancy.Robles@milwaukee.gov can be reassigned to the new email account. It is the responsibility of the employee to forward any department relevant correspondence back to the originating department after a transfer. Any exceptions to this policy needs the Chief Information Officer's approval.

Employee Responsibilities

Email remains a common method of coming into contact with computer viruses or malware, particularly via links embedded in emails or through the use of attachments. Users should exercise extreme caution before opening links or attachments contained within an email message, if the message looks suspicious. If in doubt, users should attempt to verify the validity of an email message with the sender.

The City of Milwaukee trusts that its employees will act responsibly, and always in the best interests of the taxpayers who support them and the customers who depend upon them. Each individual is responsible for complying with all applicable state and federal laws, and all City policies and standards when using the City's email system. City departments will be held accountable for the actions of individual employees to ensure that conduct meets guidelines established for appropriate use of email.

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.