Administrative Policy

Subject:	Electronic Communication Policy	Index:	2-72.02
		Page:	1 of 10
Authority:	Statute:	Issued:	05/30/2010
	Resolution:	Last Revised:	06/26/2023

Policy Purpose: This policy defines the policies and procedures that govern the District's electronic communication systems. This policy includes staff affidavit of understanding the District's policies related to electronic communication systems.

I. Policy Intention

Today's electronic and communications work environments are constantly changing. Electronic communication methods and technologies are significant factors in enabling the pace of this change.

This policy is intended to:

A. Protect the District's investment in information technology systems and safeguard the information contained within these systems.
B. Promote efficiency, clarity, and accuracy in business communications.
C. Protect the District from potential compromise of its business interests and public service responsibilities.
D. Ensure the confidentiality of information assets and other proprietary information.
E. Ensure the appropriate use and maximum benefit from electronic communications technologies.
F. Maximize the benefits of electronic communications technology without adversely affecting District operations.
G. Inform staff and authorized users of the District's right to use information technology resources to ensure that District objectives are being met.

II. Electronic Communications Technology Issues

Electronic communications technology can present the following issues for the District:

A. Create potential liability.
B. Compromise proprietary or confidential information.
C. Expose District computers to unauthorized access or viruses.
D. Create a potential for resource misuse which can inhibit and retard district productivity.

Failure to adhere to this policy and the related business practices, standards, and procedures can compromise the integrity of the information of the District, its business interests, and responsibility to the public.

Administrative Policy

Subject:	Electronic Communication Policy	Index:	2-72.02
		Page:	2 of 10
Authority:	Statute:	Issued:	05/30/2010
	Resolution:	Last Revised:	06/26/2023

III. Applicability

This document outlines the policies and procedures that govern the District's electronic communication systems (systems). This policy should be followed to ensure the proper use of the systems as defined below. All users are charged with the responsibility to use these resources in an efficient, effective, ethical, and lawful manner. This policy applies to all users of the District's computer and telecommunications resources, wherever they are located. This policy governs systems used by or with the District's systems. Violations of this policy may result in disciplinary action, including the termination of the privilege of access to some or all of the systems or termination of employment.

IV. Definitions

A. Systems

District provided computer and telecommunications resources and services including, but not limited to, host computers, file servers, desktop workstations, stand-alone computers, laptop computers, software, internal and external communications networks (e-mail and instant messaging), fax systems, networked and stand-alone photocopiers and scanners, the telephone system, cell phones, smart phones, mobile devices, and voice mail that are accessed directly or indirectly from the District's computer and telecommunications resources and services.

B. Mobile Devices

Cell phones, smart phones, handhelds, tablets, air cards, and cameras.

C. E-mail System

The computer application, and its associated data network, used to transfer a message from a sender to a designated recipient or recipients. Both the server (Microsoft Exchange) and client (Microsoft Outlook) software packages are part of the Systems.

D. E-mail Message

A communication, including notes, documents, files and attachments, transferred or stored on an e-mail system. E-mail includes messages transferred using the mail transfer features of an application, such as the send command in Microsoft Word or Excel. E-mail does not include instant messaging.

E. Electronic Communication

Content of any transfer of information by and/or through the systems. This includes all e-mail messages, all voice mail messages, file transfers, and instant messages.

F. Electronic Record
Any public record that is created, transmitted, stored, retrieved, or archived electronically rather than on paper. This includes emails, files, and images.

G. Intranet
An internal website that provide exchange and availability of information to District staff and/or their designees.

H. Internet
The global computer network over which the public World Wide Web runs. This system, for example, also carries e-mail, instant messages, podcasts, streaming audio or video, files, and graphics.

I. Social Networking
The practice of expanding the number of one's business and/or social contacts by making connections to individuals through the Internet and to promote such connections by participating in web-based groups established for that purpose.

J. Originator
The person or persons who create and send an email message.

K. Primary Recipient
All users listed in the “To” line of an email message.

L. Secondary Recipient
All users listed in the “cc” or “bcc” line of an email message.

M. Author
The person who creates a file.

N. Users
All District employees, independent contractors, temporary workers, interns, consultants, vendors, and other persons permitted to access or use the District’s computer and telecommunications resources and services. Users are considered authorized if one or both of the following have occurred:

1. An id and password have been provided.
2. Access has been furnished by the Information Technology Services (ITS) Division.

Administrative Policy

Subject:	Electronic Communication Policy	Index:	2-72.02
		Page:	4 of 10
Authority:	Statute:	Issued:	05/30/2010
	Resolution:	Last Revised:	06/26/2023

V. Guidelines

This policy provides guidelines related to electronic communication in these distinct areas.

A. E-mail Usage

1. Users of the District e-mail systems should be aware of the process of all emails coming into and leaving the District's mail system are archived for possible future audit review.
2. Users should compose and formulate e-mail messages with the knowledge that e-mail messages are business documents and public records. Originators and primary recipients of e-mail messages related to District business have responsibility for the content of their email messages.
3. Users do not have the right to expect privacy in anything that they create, send, or receive on the District's systems.
4. All lawful electronic communications, germane to District business and not otherwise prohibited by this Policy, stored, transmitted, or transferred on the District's systems are the property of the District. This does apply to incidental personal e-mails messages and/or attachments created and transmitted in the District's systems.
5. The District cannot be held liable for the loss of incidental personal email messages or attachments.
6. Electronic communications are subject to audit and review by the District.
7. Electronic communications may be obtained in the course of legal proceedings.

B. Hardware and Software

1. Use of the systems to disseminate copyrighted or licensed materials, such as articles or computer software, in violation of law is prohibited. Software and data that is obtained from the Internet must not violate the intellectual property rights of others.
2. Software and data can be imported from the Internet only if the acquisition is performed according to District purchasing policies and if the acquisition is performed according to technical standards and to applicable licensing and import/export restrictions.
3. Users may not disable or tamper with any software implemented by the District.

4. Users may only use District-approved hardware and software on District systems. The District has the right to remove nonsupported software from District systems.
5. Use of encryption technology in connection with electronic communication is permitted only in accordance with District Policy.
6. Employees should safeguard the electronic equipment assigned to them. Employees who are negligent in this duty may be accountable for any loss or damage that may result to the equipment to the extent permitted by State law. If District information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the employee must contact the Risk Management Department and the ITS Division.

C. Internet, Intranet, and Social Networking Usage

1. Material on the Internet does not have to be illegal or patently offensive to be deemed inappropriate for the workplace. Specifically, while limited personal use of Internet and e-mail facilities is allowable as outlined in this Policy, excessive access to non-District business related sites (sports, financial, vacation planning, consumer products, entertainment, etc.) is not allowed.
2. Use of web publishing software or the development, administration, or operation of websites on the systems which are not related to District business is prohibited without prior consent of the Director of Information Systems.
3. The Internet must be accessed using only the standard Internet access mechanisms provided by the District.
4. Employees releasing confidential information, whether or not the release is inadvertent, may be subject to disciplinary action.

D. Personal Use of the Systems

1. Proper business judgment and discretion should be exercised when using any electronic communications resources. Inappropriate, potentially offensive, improper, or harassing communications or communications which contain obscenity, vulgarity, sexually explicit content, or profanity is prohibited.
2. The systems shall not be used at any time for any illegal activity or any activity that is in violation of any other District policy. Users shall not send messages that are fraudulent, harassing, indecent, profane, intimidating, scandalous, defamatory, libelous, or obscene.

2. Any user who receives material that is in any way offensive or falls in the categories identified above should immediately report the incident to the ITS Division and/or the Risk Management Department.
3. In addition, such materials may not be archived, stored, distributed, edited, or recorded using District systems.
4. District systems may not be used for personal gain, religious causes, political causes, the solicitation of commercial ventures, or other non-job-related solicitations.
5. The use of District systems for personal purposes during work hours is strictly prohibited except as provided below:
    a. The reasonable and limited use of the systems, such as phone, e-mail, or instant messaging, for the preparation and transmission of personal electronic messages is permitted during work hours, as long as such use does not interfere with completion of the employee's work, disrupt use of the systems, or otherwise violate this policy.
    b. Employees may use the District's Internet for nonbusiness research or browsing during their designated lunch time, or outside of work hours, provided that such use does not interfere with official duties, that time spent at such activities is reasonably limited, and that all other District and departmental usage policies are adhered.
    c. The reasonable and limited use of social networking (Facebook, Twitter, YouTube, etc.) services, outside of the scope of District business is allowed within the limits of the above stipulations.
6. The use of the Systems for non-business-related mass mailings is prohibited. Such mailings compromise District systems and the District's ability to provide business-related mailings that are appropriate. Mass mailings from District-approved committees, such as Employees' Connection, are exempt from this requirement. The Director of Information Technology Systems has the final determination as to the authorization of such mass mailings.
7. Use of the systems to send or receive communication or material that does not accurately reflect the sender's identity is prohibited. Use of an anonymous re-mailer or similar system to send or receive e-mail messages is prohibited.

E. Remote access is addressed under Administrative Policy 2-72.19, Remote Access.
F. Mobile device use is addressed under Administrative Policy 2-72.20, Mobile Device Acceptable Use Policy.

VI. Electronic Records Retention

Any electronic communication related or germane to District business, contracts, schedules, budgets, policies, or other matter that is received or generated on District systems is a public record, subject to disclosure under Wisconsin's Public Records Law and statutory retention requirements.

Since e-mail and other electronic communication related to District business are public records, they must be managed and maintained in accordance with applicable records management laws, policies, and procedures. As with any other type of public record, users must be aware of the District record retention and disposal requirements which are outlined in the above referenced policies.

VII. Security

A. Adherence to Security Controls

Any employee, contractor or other entity who makes use of District communication systems is required to adhere to any and all security controls. These controls apply to many areas including but not limited to email, web browsing, data, access, malware, security training, incident response or monitoring. These controls are documented and are subject to change without notice.

B. Regular Monitoring

Contents of electronic communications or web browsing might be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. The District reserves the right to disclose any electronic messages to law enforcement officials without prior notice to any employees who might have sent or received such messages. Users should structure their electronic communications recognizing the fact that the District has the right to examine the content of electronic communications. Because all messages are records the District reserves the right to access and disclose any message sent over its

electronic messaging systems. The ITS Division and Department Supervisors have the right request a review of the electronic communications of the employees they supervise to determine whether there have been any breaches of security, violations of company policy, or unauthorized actions on the part of the employee.

An account may be inspected, monitored, or disabled when any of the following is true but not limited to:

1. General usage patterns indicate that an account is likely to be responsible for activity that is in violation of federal, state, or local law, or District policy.
2. There is a credible report of a violation of policy or law.
3. It is necessary, in the judgment of District administration, to do so to protect the District from liability.
4. The District receives a public records request, a valid subpoena, or a litigation discovery request.

C. No Expectation of Privacy

As a result of the monitoring privileges defined herein, users should expect that the District might access all information created, transmitted, downloaded, received, or stored in District computers at any time, without prior notice. Users should not assume that they have an expectation of privacy or confidentiality in such messages or information (whether or not this content is password protected), or that deleted messages are necessarily removed from the system.

VIII. General Policy Provisions

A. Guidelines for Users – Summary

While the guidelines described in each section of this policy dictate how District employees can and cannot use the District's systems, these guidelines cannot cover every conceivable situation; common sense, organizational responsibility, professional courtesy will still be required.

Material on the Internet does not have to be illegal or patently offensive to be deemed inappropriate for the workplace. Specifically, while limited personal use of the Internet and e-mail services is allowable as outlined in this Policy, excessive access to non-

District related sites (sports, financial, vacation planning, consumer products and entertainment, social networking sites to name a few) is not allowed.

The guidelines outlined here are intended to cover reasonably foreseeable circumstances, but other uses of the systems could violate District work rules or administrative policies. As with any violation of work rules or administrative policies, inappropriate use of the systems may be grounds for disciplinary action up to and including discharge.

B. Violations

Violations of this policy or any related policies or standards may be grounds for disciplinary action up to and including termination of employment for District employees or termination of the contract(s) and services of a temporary worker, intern, external consultant, vendor, or contractor. Some actions that are violations of this or other policies could also result in civil or criminal liability for the user.

C. Reporting Unauthorized Use/Access

Users should report any potential, suspected or actual violations of this policy or any related District policies to their immediate supervisor, division director, the Human Resources Department, or the Director of Information Technology Systems or his/her designee, as appropriate.

Questions related to these policies and their application should be directed to the Director of Information Technology Systems or his/her designee.

IX. Acknowledgment of Electronic Communications Policy

This form is used to acknowledge receipt of, and compliance with, the Milwaukee Metropolitan Sewerage District's Electronic Communication Policy.

Signature

By signing below, I agree that I have received and read a copy of the Electronic Communication Policy and understand the same.

Employee Signature: Gaurav Mittal

Administrative Policy

Subject:	Electronic Communication Policy	Index:	2-72.02
		Page:	10 of 10
Authority:	Statute:	Issued:	05/30/2010
	Resolution:	Last Revised:	06/26/2023

Employee Name: Gaurav Mittal

Date: 09-13-2023

Department:

Return this page only to the Human Resources Department.