POLICY TITLE	Acceptable Use Policy	**DOCUMENT ID**	ADMIN-RM-0205.03
OWNER	Vice President of Business Administration	**CREATION**	07.27.2021
STANDARDS AND REGULATIONS	**COA:** RPM 4, RPM 4.04, RPM 5, RPM 5.01, RPM 5.02, RPM 8.03 **Admin Code:** **Statute:**	**RENEWAL DATE**	09.2028
RELATED OMC POLICIES / PROCEDURES	Network Access and Authentication Policy; Social Media Use Policy/Procedure; Password Policy; Artificial Intelligence Policy; Artificial Intelligence Procedure; Microsoft SharePoint Procedure; Microsoft Teams Digital Headquarters Procedure; Microsoft Teams Video Conferencing Procedure; Asana Project Management Procedure	**LAST MODIFIED/ APPROVAL**	07.2026 – Chief Financial Officer
APPLICABLE TO	1 - All Staff 8 - Volunteers	**EXPERT REVIEW**	07.2021-Nelson Mullins

PURPOSE

This policy's purpose is to detail the acceptable use of information technology resources for the protection of all parties involved. Since inappropriate use of systems exposes One More Child to risk, it is important to specify exactly what is permitted and what is prohibited. This policy explains how information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using resources. Questions on what constitutes as acceptable use should be directed to the user's supervisor.

FORMS AND REFERENCE DOCUMENTS

Title	Description

POLICY

Email Use

Personal usage of email systems should be reasonable and limited. Email systems are intended primarily for business communications, but personal use is permissible provided the privilege is not abused.

- The following are never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive but is included to provide a reference frame for prohibited activities.
- The user is prohibited from forging email header information or attempting to impersonate another person
- It is policy not to open email attachments from unknown senders or when such attachments are unexpected
- Email systems were not designed to transfer large files, so emails should not contain attachments of excessive file size
- Non-One More Child (OMC) email accounts should not be used for business related emails

Confidentiality

Confidential data, whether stored on the network or within a third-party hosted web application database, must not be:

- Shared or disclosed to non-staff without permission from the department head
- Posted on the internet or any publicly accessible systems
- Transferred in any non-secure manner. Please note that this is only a brief overview of how to handle confidential information, and that other program or departmental specific policies may refer to the proper use of this information in more detail.

Network Access

The user should make reasonable efforts to avoid accessing network data, files, and information that are not related to the user's job function. The existence of access capabilities does not imply permission to use this access. If the user encounters sensitive information that should have restricted access, the user should report the discovery to the supervisor who will be responsible for advising the appropriate individuals and/or managed service provider.

Unacceptable Use
The following actions shall constitute unacceptable use of the network. This list is not exhaustive but is included to provide a frame of reference for activities deemed unacceptable. The user may not use the network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to OMC
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media
- Engage in activities that cause an invasion of privacy
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace
- Make fraudulent offers for products or services
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other information gathering techniques when not part of staff's job function
- Install or distribute unlicensed or "pirated" software
- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations

Overuse
Actions detrimental to the computer network or other OMC resources, or that negatively affect job performance, are not permitted.

Web Browsing
OMC recognizes that the internet can be useful for personal and professional purposes. Personal usage of computer systems to access the internet is permitted but should be reasonable and limited. Usage should follow pertinent guidelines found elsewhere in this document and be judicious to avoid having a detrimental effect on OMC or on the staff's job performance.

Copyright Infringement
The computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner:

- Copying and sharing images, music, movies, or other copyrighted material using Peer-to-Peer file sharing or unlicensed CDs and DVDs
- Posting or plagiarizing copyrighted material
- Downloading copyrighted files which staff have not already legally procured

This list is not meant to be exhaustive. Copyright law applies to a wide variety of works and applies to much more than is listed above.

Peer-to-Peer File Sharing
Peer-to-Peer networking is not allowed on the network under any circumstances.

Monitoring and Privacy
The network, all resources, and all data transmitted or received through them, are the exclusive property of OMC. Users, including all staff, interns, volunteers, contractors, vendors, partners, associates, and any others accessing and/or using OMC's systems, should have no expectation of privacy in any communication over the network or resources. Such use may include transmission and storage of files, data, and messages.

OMC reserves the right to monitor any, and all, use of the network systems, intercept, and/or review all data transmitted, received, or downloaded over the system. To ensure compliance with policies, this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media. Any individual who is given access to the system is hereby given notice that OMC will exercise this right periodically, without prior notice and without prior consent of the staff.

OMC's interests in monitoring and intercepting data include, but are not limited to:

- Protection of trade secrets, proprietary, and similar confidential commercially sensitive information (i.e., financial or sales records/reports, marketing or business strategies/plans, product development, customer lists, patents, trademarks, etc.)
- Managing the use of the computer system
- Assisting staff in the management of electronic data during periods of absence

No individual should interpret the use of password protection as creating a right or expectation of privacy. To protect everyone involved, no one can have a right or expectation of privacy with regards to the receipt, transmission, or storage of data on the Voicemail/Email/Internet system. Any staff who violate these policies will be subject to corrective action, up to and including termination of employment. If necessary, OMC will also advise law enforcement officials of any illegal conduct.

Artificial Intelligence
For specific requirements and guidance regarding the appropriate use of artificial intelligence (AI) tools, please refer to the Artificial Intelligence Policy and Procedure.

Bandwidth Usage
Excessive use of bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity, or performance must be performed during times of low organization-wide usage.

Personal Usage
Personal use of computer systems should be reasonable and limited. The computer systems are intended primarily for business use, but personal use is permissible provided the privilege is not abused.

Remote Desktop Access
Use of remote desktop software and/or services is allowable if it is provided by OMC. Remote access to the network must conform to the Network Access and Authentication Policy.

Circumvention of Security
Using OMC-owned/provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly, taking any actions to bypass or circumvent security is expressly prohibited.

Use for Illegal Activities
No OMC-owned/provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of terrorism
- Identity theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statues
- Downloading, storing, or distributing copyrighted material

OMC will take all necessary steps to report and prosecute any violations of this policy.

Non-OMC-Owned Equipment
The introduction of non-OMC-provided equipment on the network without prior notification to the Managed Service Provider or appropriate personnel is prohibited.

Personal Storage Media
Personal storage devices represent a serious threat to data security and are expressly prohibited on the network.

Software Installation
Installation of non-OMC-supplied programs and apps on the OMC system or OMC computers is expressly prohibited.

Reporting of Security Incident
If a security incident or breach of any security policies is discovered or suspected, the user should immediately notify the appropriate supervisor and notify the Vice President of Business Administration. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.)
- Suspected virus/malware/Trojan infection
- Suspected mirroring, cloning, or hacking of phones or computers
- Loss or theft of any device that contains OMC information
- Loss or theft of identification badge or keycard
- Any attempt by any person to obtain a user's password over the telephone or by email
- Any other suspicious event that may impact information security

Users must treat a suspected security incident as confidential information and report the incident only to the appropriate supervisor.

Users must not withhold information relating to a security incident or interfere with an investigation.
OMC will abide by all applicable contractual and regulatory requirements, including state and federal statutes and administrative code.

Enforcement
Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of property (physical or intellectual) are suspected, OMC may report such activities to the applicable authorities.