POLICY TITLE	Network Access and Authentication Policy	**DOCUMENT ID**	ADMIN-RM-0207.03
OWNER	Vice President of Business Administration	**CREATION**	07.27.2021-Board
STANDARDS AND REGULATIONS	**COA:** RPM 4, RPM 5, RPM 5.01, RPM 5.02 **Admin Code:** **Statute:**	**RENEWAL DATE**	09.2028
RELATED OMC POLICIES / PROCEDURES	Acceptable Use Policy, Social Media Use Policy, Password Policy, Guest Access Procedure, Personally Owned Devices Policy; Email Encryption Procedure	**LAST MODIFIED/ APPROVAL**	09.2026 – Chief Financial Officer
APPLICABLE TO	1 – All Staff 8 - Volunteers	**EXPERT REVIEW**	07.2021-Nelson Mullins

PURPOSE

Consistent standards for network access and authentication are critical to One More Child's information security and are often required by regulations or third-party agreements. Any user accessing the computer systems can affect the security of all users of the network. An appropriate Network Access and Authentication policy reduces the risk of a security incident by requiring consistent application of authentication and access standards across the network.

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the network are authenticated in an appropriate manner, in compliance with standards, and are given the least amount of access required to perform the job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

FORMS AND REFERENCE DOCUMENTS

Title	Description
Termination Checklist form	ADP Forms Library

POLICY

Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across One More Child (OMC). The following best practices apply to account use:

- Accounts must be created using a standard format (firstname.lastname is the present adopted format)
- Accounts must be password protected (refer to the Password Policy for more detailed information)
- User accounts must not be given administrator or 'root' access unless this is necessary to perform the job function
- All individuals requiring access to confidential data must have an individual, distinct account. These accounts may be subject to monitoring or auditing by the Managed Service Provider at the discretion of OMC, or as required by applicable regulations or third-party agreements.
- Occasionally guests will have a legitimate business need for access to the OMC network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, is to be restricted as per the Guest Access Procedure and will be revoked upon cessation of need.

Account Termination

It is important to communicate when a staff member has left or will soon leave OMC so their account can be disabled, and incoming emails can be redirected to an appropriate staff member. The Termination Checklist form is designed for reporting this information and should be submitted promptly to Human Resources. The Human Resources Department will coordinate with the Administration Department so that the Managed Service Provider can be notified of the account changes needed in a timely manner.

Authentication
User machines must be configured as per accepted industry standards for corporate management and security. This includes being enrolled in our Mobile Device Manager. Personally owned devices are covered by the Personally Owned Devices Policy.

Use of Passwords
When accessing the network locally, username and password or Personal Identification Number is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the Password Policy.

Remote Network Access
Remote access to the network can be provided for convenience to users; however, this comes at certain risk to security. For that reason, OMC performs additional scrutiny of users remotely accessing the network. Both on-site and remote access must adhere to the same standards communicated in the organization's information technology policies and procedures.

Idle Computers
Whenever a computer is left unattended, the screen should be locked to prevent a malicious user, curious staff, or intruder from accessing network resources through the idle computer.

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.