POLICY TITLE	Password Policy	**DOCUMENT ID**	ADMIN-RM-0208.03
OWNER	Vice President of Business Administration	**CREATION**	07.27.2021
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; Network Access, and Authentication Policy; Password Procedure; Guest Access Procedure; Data Retention for Terminated Employees Procedure	**LAST MODIFIED/ APPRVOAL**	07.2026 – Chief Financial Officer
APPLICABLE TO	1 – All Staff 8 - Volunteers	**EXPERT REVIEW**	07.2021-Nelson Mullins

PURPOSE

The Password Policy, in conjunction with the associated Password Procedure, is designed to address and provide guidance related to the use of passwords and Personal Identification Number codes.

FORMS AND REFERENCE DOCUMENTS

Title	Description

POLICY

Password Configuration & Standards
One More Child (OMC) shall follow accepted industry standards for network security that include a combination of passwords, Personal Identification Number codes, and biometric data along with multi-factor authentication. Password construction details and related password creation specific instructions are provided in the Password Procedure.

Confidentiality
Passwords and Personal Identification Number codes should be considered confidential data and treated with the same discretion as any of OMC's proprietary information. Whatever method utilized to store or keep track of password information must be secure and not easily accessed.

Incident Reporting
Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving passwords to the appropriate supervisor and the Vice President of Business Administration who will be responsible for reporting the incident to any other appropriate parties. Any request for passwords or Personal Identification Number codes over the phone or email, whether the request came from someone in authority or not, should be reported.

When a password is suspected to have been compromised, the user(s) will be instructed to change all passwords and Personal Identification Number codes.

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.