PROCEDURE TITLE	Guest Access Procedure	**DOCUMENT ID**	ADMIN-RM-0248.02
OWNER	Vice President of Business Administration	**CREATION**	05.30.2024
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	Password Policy; Network Access and Authentication Policy	**LAST MODIFIED/ APPROVAL**	07.2026 – Chief Financial Officer
APPLICABLE TO	1 – All Staff 8 - Volunteers	**EXPERT REVIEW**	

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 Guest Access procedure reduces the risk of a security incident by requiring consistent application of authentication and access standards across the network.

The purpose of this procedure is to describe the steps that must be taken to ensure that guests 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 their job function. This procedure specifies what steps are taken for appropriate use of network accounts and authentication standards.

FORMS AND REFERENCE DOCUMENTS

Title	Description

PROCEDURE

Types of Guest Access
There are three approved guest access categories – Interns, Long-term or Repeat Volunteers, Short-term Volunteers.

- **Network Access for Interns**
  - Interns will be assigned a personal account on One More Child's (OMC) network with access to necessary data in their department's SharePoint site. Interns are subject to all policies and procedures included in OMC's cohesive set of security policies. Interns will be required to complete the same training regarding network security and HIPAA compliance as an OMC employee. This account will remain in effect until termination of the internship.
- **Network Access for Long-term or Repeat Volunteers**
  - Volunteers who will be serving regularly for extended periods of time without a material gap in service will be assigned a personal account on OMC's network with access to log in to OMC computers for internet access and printing services only. These volunteers are subject to all policies and procedures included in OMC's cohesive set of security policies. Long-term or Repeat volunteers will be required to complete the same training regarding network security and HIPAA compliance as an OMC employee. This account will remain in effect until a material gap in service occurs.
- **Network Access for Short-term Volunteers**
  - Volunteers serving on a short-term or irregular basis that require access to OMC's network will utilize a shared log-in account for computer access purposes. This shared account will only allow access to the internet. These volunteers are subject to all policies and procedures included in OMC's cohesive set of security policies. Short-

term volunteers will be required to receive verbal instruction regarding network security and HIPAA compliance.
    - This type of access requires the OMC Supervisor over that area to maintain a log of computer access that includes the name of the volunteer, the time(s) of access, and a brief purpose for the access. This log shall be maintained for at least two years and is subject to review or auditing by the Managed Service Provider at the discretion of OMC, or as required by applicable regulations or third-party agreements.

Data Access for Interns and Volunteers
Interns will have access to SharePoint data as directed by the Executive Director over that area where the intern is serving. This access is equivalent to the access provided to OMC employees through their network login credentials.

Volunteers needing access to data will have to utilize the sharing feature of SharePoint. This will be granted case-by-case through the normally established procedures for SharePoint by the supervisor over the service area. This temporary share will be subject to the designated time limits established through the SharePoint site or as amended by the supervisor at the time of the share.

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.