PROCEDURE TITLE	Client Confidentiality in the Workplace Procedure	**DOCUMENT ID**	PROG-0206.02
OWNER	Vice President of Program Operations	**CREATION**	07.27.2021
STANDARDS AND REGULATIONS	**COA:** CR 2, PRG 1.05, RPM 5, RPM 5.01, 5.02 **Admin Code:** FAC 65C-45.003 **Statute:** FL 39.201, FL 39.202; FL 415.513	**RENEWAL DATE**	02.2027
RELATED OMC POLICIES / PROCEDURES	Client Confidentiality Policy, Client Records-Release of Information Policy; Client Case Notes and Documentation Procedure; Client Rights and Responsibilities Policy/Procedure; Termination Policy; Email Encryption Procedure; Client Photographs and Videos Procedure; Child Protection Policy/Procedure	**LAST MODIFIED/ APPROVAL**	1.2025/Chief Operating Officer
APPLICABLE TO	2 – All Programs	**EXPERT REVIEW**	

PURPOSE

This procedure protects the rights and privacy of children and families in gathering and disseminating information and in all promotional activities. It ensures the confidentiality and privacy of clients by providing a secure work environment to protect information. This procedure will ensure that One More Child is following all applicable statutory requirements pertaining to confidentiality.

FORMS AND REFERENCE DOCUMENTS

Title	Description
Confidentiality and Nondisclosure Agreement	ADP (at on boarding)
Termination Checklist	ADP
HIPAA Privacy & Security Manuals	OMC Central

PROCEDURE

The security and protection of client information in the One More Child (OMC) work environment is paramount. The collective effort to ensure the privacy and security of confidential information upholds the OMC core values, demonstrates respect for our clients, and supports compliance with state and federal laws.

All information regarding past, present, and future clients and/or their relatives is considered to be confidential and covered by these procedures. Upon hiring and during the onboarding process, staff will sign a "Confidentiality and Nondisclosure Agreement" acknowledging their understanding.

Need-to-Know/Minimum Necessary

- Among staff, volunteers, and organizations, client information should only be shared on a need-to-know basis. Staff/volunteers are not to discuss a client (even the existence of a client) with anyone outside of the authorized operations teams. Staff should ask "Do I need to access this information in order to do my job?" If client information is not necessary to perform job functions, it should not be accessed.
- Under no circumstances will staff share information about past, present, or future clients outside of their responsibilities and duties as a staff/volunteer working on a specific case. If approached by an individual seeking information outside these parameters, staff/volunteers will decline to offer information and direct the individual to the appropriate (OMC) staff.
- Staff/volunteers will practice extreme diligence in sharing information only in staff secure areas. Staff/volunteers will not discuss clients in common areas of the facility where members of the public may hear such information.
- OMC volunteers are also subject to the need-to-know rule. Staff who oversee the work of volunteers will share minimal information with volunteers about specific clients, sharing information only to the extent that it impacts the scope of the volunteer's work with the client. For example, a volunteer who tutors a child may be told that the child is experiencing

difficulty in school performance, but the same volunteer is not to be told personal information about the client, their family, the status of the case, or the circumstances that brought the family under the supervision of the organization.
- Staff will continue to caution caregivers to share only need-to-know information with other caregivers.

Workplace Confidentiality

To ensure the privacy and confidentiality of this information, the following steps are taken:

- Documents containing client-specific information, including case files, are stored in a locked area when outside of the presence of staff.
- Digital/electronic client files and information are secured by data security systems. Data will be limited to information that is necessary and appropriate for services being provided and accessible only to appropriate personnel.
    - Staff are to utilize password protection to access client information and log off the system before walking away from their computers.
    - Computer monitors should be positioned to mitigate casual observation. Always secure phones/tablets.
    - Procedures regarding staff termination process and removal of access to confidential client information in all forms, are to be followed per proper human resources termination procedures and applicable programmatic termination protocols.
    - Ensure that sensitive client information is encrypted when being sent via email by utilizing the proper steps outlined within the Email Encryption Procedure.
- When retrieving voice mail messages or discussing client-specific information, staff should refrain from using speakerphone feature (cell or land line phones) when in open areas, hallways, conference rooms, and cubicles.
- When meeting virtually or through telehealth mechanisms with clients, their families, external service providers, other staff, or anyone else regarding client-specific information, staff are to ensure that their conversations are held in a confidential setting not frequented by the public and take place in soundproof areas when possible.
- Staff should use discretion when leaving their desk or office unattended for even a short period of time. If there are confidential documents or sensitive client information open on a computer and/or laid out on a desktop – those files should be locked in a cabinet or locked behind a closed door prior to stepping away. Case files and other documents with client-specific information cannot be left in open cubicles unattended, unlocked offices, or in other open areas (i.e., on a table, printer, or copy machine) when outside the presence of staff.

Remote Work

Staff working remotely from home are to adhere to the same professional policies and procedures protecting client privacy and confidentiality. As when working in an office, client confidentiality must be guarded when working remotely. The following is to occur:

- Do not discuss clients with household members.
- Log off the computer at the end of each workday.
- Locate a workspace at home which allows for privacy.
- Do not throw any paperwork in the trash which may include client information. Either shred these items or collect and bring to the main office to shred when possible.
- If physical case files are brought home, have locking/portable file cases available.

Media Privacy

Capturing/duplicating of any client information or client image via an unauthorized electronic device (such as, but not limited to personal cameras, video cameras, or cell phones) is prohibited unless staff have followed both the Client Photographs and Video Procedure, and Photography Guidelines Procedure.

Training

OMC staff, volunteers, and caregivers will receive appropriate training as needed on confidentiality and ethical standards.

Compliance

Staff are to report any breach or potential breach of client information to their supervisor and Risk Management. OMC will abide by applicable contractual and regulatory requirements regarding any breach of information, to include state and federal statutes and administrative code.

Penalties

A person who knowingly and willfully makes public disclosures of any confidential information to any unauthorized person is subject to the penalty provisions of §415.513, F.S. (second degree misdemeanor).