The Moore Center
Creating opportunities for a good life.℠

SMS Text Messaging Policy

1. Purpose

This policy establishes requirements for the appropriate use of text messaging in support of The Moore Center (MCS) "the Agency," operations while protecting the privacy, confidentiality, and security of information and ensuring compliance with applicable laws and regulations.

2. Scope

This policy applies to all employees, contractors, interns, volunteers, and other workforce members of MCS who use text messaging to communicate with individuals receiving services, guardians, providers, vendors, community partners, or other business contacts on behalf of the Agency.

3. Policy Statement

MCS permits the use of text messaging for legitimate business purposes, including routine communication and service coordination. All text communications must be conducted through the agency-approved platform whenever possible. Employees must protect confidential information and comply with HIPAA, New Hampshire confidentiality requirements, and all Agency privacy and security policies. Text messaging shall be used in a manner that safeguards individual privacy and maintains professional standards of communication.

4. Definitions

- **Approved platform** means the Agency-authorized system used for business texting and related documentation.
- **Client-related text communication** means any text message concerning an individual receiving services, a guardian, services provided or coordinated by the Agency, or information connected to care, support, billing, operations, or service coordination.

- **Confidential information** includes PHI, PII, personnel information, financial information, proprietary Agency information, and any other non-public information that is protected by law, regulation, contract or Agency policy.

5. Policy Requirements

a. Employees must use the agency-approved platform for text communication whenever possible. Text messaging may also be used for routine business purposes, including verification messages, one-time passcode (OTP), multi-factor authentication (2FA), advocacy-related communications, emergency alerts, safety notifications, surveys, feedback, service notices, appointment reminders, scheduling, billing, payment alerts, security alerts, internal staff communications, employee notifications and other general updates.

b. Protected Health Information (PHI), personally identifiable information (PII), and other confidential information must not be transmitted through personal devices, personal accounts, or unapproved messaging applications.

c. Employees must verify recipient information before sending text messages, confirm that the message is intended for that recipient, and limit message content to the minimum necessary for the business purpose(s).

d. Text messages must be professional, accurate, and limited to Agency business.

e. Text messaging must not be relied upon as the sole method of communication during emergencies, crisis intervention situations, or circumstances requiring an immediate response. Employees must follow established emergency communication procedures and direct individuals to appropriate emergency or crisis resources when immediate assistance is required.

f. Clients, guardians, and other recipients must be informed before receiving text communications that texting may have privacy and security limitations, that message and data rates may apply, that texting is not appropriate for emergencies, and that they may opt out of receiving text messages at any time. The Agency must document any required consent, communication preferences, and opt-out requests in accordance with applicable procedures. Text messages to clients, guardians, or other external recipients shall be sent only after any required consent has been obtained and documented in accordance with applicable laws, regulations, Agency procedures, and communication preferences.

g. Text communications that constitute business records, clinical records, financial records, or other official Agency records must be retained, archived, or incorporated into the appropriate Agency system in accordance with record retention schedules, legal requirements, and regulatory obligations.

h. Lost, stolen, or compromised devices used for Agency communications must be reported immediately in accordance with Agency security procedures.

i. Suspected misdirected messages, unauthorized disclosures, lost or stolen devices, compromised accounts, or other texting-related privacy or security incidents must be reported immediately through the Agency's established incident reporting process. Employees must not delete, alter, or conceal relevant messages or device information unless instructed through the Agency's approved incident response procedure.

j. Employees using personal devices for Agency-approved texting activities must comply with all Agency mobile device security requirements, including password protection, encryption, remote wipe capabilities where applicable, and prompt reporting of device loss or compromise.

k. Failure to comply with this policy may result in disciplinary action, up to and including termination, and may subject the individual to legal or regulatory consequences.

l. Communications conducted through Agency-approved platforms may be monitored, audited, retained, or reviewed by the Agency for compliance, security, operational, legal, or regulatory purposes, consistent with applicable laws.

m. Workforce members must maintain reasonable safeguards when sending or receiving text messages, including securing devices with passwords or biometric authentication, enabling automatic screen locks, and avoiding the display of confidential information where it may be viewed by unauthorized persons.

6. Roles and Responsibilities

Employees are responsible for using approved communication tools, protecting confidential information, verifying recipients before sending messages, and reporting suspected privacy or security incidents immediately. Supervisors are responsible for reinforcing this policy, monitoring compliance within their teams, and escalating concerns to the appropriate Agency leadership. The Privacy Officer, Security Officer, and/or

designated compliance lead is responsible for maintaining this policy, reviewing incidents, and updating requirements as laws, technology, and Agency procedures change.

7. Training and Acknowledgement

Workforce members who use text messaging for Agency business must complete any required training on this policy and applicable privacy, security, and communication procedures. The Agency may require periodic acknowledgement of this policy and may restrict texting access for individuals who have not completed required training or who fail to comply with this policy.