

PRIVACY & CONFIDENTIALITY POLICY

McMinnville Warren County Senior Center

Purpose and scope. The McMinnville Warren County Senior Center is committed to treating people with respect and protecting personal information entrusted to the Center. This policy applies to everyone who interacts with the Center or whose information the Center receives, including members and program participants, employees, volunteers, visitors, caregivers and family members, vendors, contractors, community partners, and other individuals. It applies to information in paper, electronic, verbal, photographic, and other formats.

1. Information We May Collect

Depending on the relationship and services involved, the Center may collect or maintain names, addresses, telephone numbers, email addresses, emergency contacts, attendance and meal-program records, transportation details, eligibility or referral information, payment and donation records, employment or volunteer records, incident and complaint reports, photographs or videos, and other information reasonably needed to operate programs, provide services, ensure safety, or meet reporting requirements. The Center should collect only information reasonably necessary for the purpose.

2. How Information Is Used

Information may be used to register people for activities, communicate schedules and closures, coordinate transportation and services, contact emergency contacts when appropriate, manage meals and attendance, process payments or donations, administer employment and volunteer activities, respond to concerns, document incidents, evaluate programs, meet grant or contract requirements, and comply with applicable laws.

3. Confidentiality Expectations

Employees, board members, and volunteers must protect confidential information learned through their role and use it only for authorized Center purposes. Members, visitors, caregivers, vendors, and guests are expected to respect others' privacy and not photograph, record, publish, or share another person's private information without permission, except as allowed by law or Center rules. Personal information should not be discussed in public areas or shared with people who do not have a legitimate need to know.

4. Health, Emergency, and Sensitive Information

Health-related details, disability information, emergency contacts, accommodation requests, and other sensitive information must be handled discreetly. Access should be limited to authorized people who need the information for safety, service coordination, or another legitimate purpose. The Center does not represent that all records it maintains are protected by HIPAA; applicable privacy obligations depend on the Center's role and the records involved.

5. Photographs, Videos, Audio, and Social Media

The Center may photograph or record activities for newsletters, displays, websites, social media, or program documentation. When an identifiable person's image or recording is to be used for publicity, the Center should obtain permission or a signed release when appropriate. Anyone who does not wish to be photographed should tell Center staff, who will make reasonable efforts to respect that request. Visitors and participants should not record or post identifiable images, conversations, or personal information about others without permission, unless otherwise permitted by law or expressly authorized by the Center.

6. Sharing and Disclosure of Information

The Center does not share personal information casually or for unrelated purposes. Information may be shared with authorized service providers, partner agencies, funders, auditors, or government entities when reasonably necessary to provide services, coordinate referrals, verify eligibility, document expenses or outcomes, meet program requirements, respond to emergencies, or comply with law. The Center should limit shared information to what is reasonably necessary when practical. Information may also be disclosed when required or permitted by law. The Center cannot guarantee confidentiality when disclosure is legally required or necessary to address an immediate safety concern.

7. Secure Storage, Access, and Disposal

Paper records should be kept in secured areas, and electronic records should be protected by appropriate passwords and access controls. Records should not be left where unauthorized people can view them. Confidential documents should not be taken off-site, copied, or sent through personal accounts without authorization. Records must be retained and disposed of according to applicable law, funding agreements, contracts, and the Center's record-retention practices. When disposal is permitted, paper records should be shredded or securely destroyed and electronic records securely deleted when appropriate.

8. Privacy Incidents and Concerns

Anyone who becomes aware of lost records, unauthorized access, accidental disclosure, inappropriate recording, or another privacy concern should promptly report it to the Executive Director or designated Center representative. The Center will review the concern as promptly and discreetly as practical and determine whether corrective action or notification is required. Retaliation against someone who raises a good-faith concern is not permitted.

9. Individual Questions and Requests

A person may ask the Center what information it maintains about them or raise a concern about how information has been used. The Center will consider the request and respond as appropriate, subject to applicable law, record-retention obligations, and the rights or privacy of others. Requests should be directed to the Executive Director.

10. Administration and Review

The Executive Director or designated representative is responsible for communicating this policy to relevant staff and volunteers, supporting appropriate privacy practices, and bringing concerns forward for review. The policy should be reviewed periodically and updated as needed. Where applicable law, a funding agreement, or a contract imposes a stricter requirement, that requirement must be followed.

This policy is provided for public information. It is a general statement of the Center's privacy practices and may be updated as programs, practices, or applicable requirements change.

Est. Date: 10/15/2026