centrexIT™

TOOLKIT · 01 OF 10

Staff AI Acceptable Use Policy

A starting-point policy template for elder-serving organizations. Adapt the bracketed sections to fit your org and adopt formally through your normal governance process.

BEFORE YOU ADOPT THIS

This template is provided as a starting point. It is not legal advice. Have your policy reviewed by counsel familiar with your state's privacy law, applicable funder requirements (HRSA, AAA, HHS, state Medicaid), and your insurance carrier before adoption.

Sections in **[BRACKETS]** require your organization to fill in. Examples are provided in italics.

1. Purpose

[ORGANIZATION NAME] serves older adults who rely on us to protect their personal, medical, and financial information. AI tools — chatbots, image generators, transcription services, productivity assistants — can improve our work, but they also create new risks for the people we serve.

This policy establishes how staff, volunteers, contractors, and board members may use AI tools when conducting business on behalf of the organization. It is designed to support thoughtful AI use, not to prohibit it.

2. Scope

This policy applies to:

- All employees of [ORGANIZATION NAME], full-time and part-time
- All volunteers and interns acting on behalf of the organization
- All contractors, vendors, and consultants with access to client information
- All board members and committee members

This policy applies regardless of device — personal phone, organization laptop, home computer — whenever an individual is acting on behalf of the organization or handling information that belongs to the organization or its clients.

3. Definitions

AI Tool

Any software service that uses artificial intelligence, machine learning, large language models, or generative algorithms to produce text, images, audio, video, summaries, recommendations, or decisions. Examples include but are not limited to ChatGPT, Claude, Gemini, Copilot, Midjourney, ElevenLabs, Otter, Fireflies, and AI features built into existing tools like email, search, or productivity software.

Client Information

Any information about an individual served by [ORGANIZATION NAME], including name, date of birth, address, phone, Social Security number, Medicare/Medicaid number, health status, medications, financial situation, family relationships, case notes, photographs, intake forms, or any other identifying or sensitive detail. Client information remains client information whether spoken, typed, photographed, or summarized.

Public AI Tool

Any free or consumer-tier AI service where prompts and inputs may be used by the provider to train future models or are not subject to a business-grade data use agreement. Examples: free ChatGPT, free Claude, free Gemini, public image generators.

Approved Enterprise AI Tool

An AI tool that [ORGANIZATION NAME] has formally approved for business use under a written agreement that prohibits the provider from using inputs to train models, includes data residency commitments, supports audit logs, and meets the organization's encryption and access requirements. The current list of approved enterprise AI tools is maintained at [LINK / LOCATION].

4. Approved Uses

Staff and volunteers may use Approved Enterprise AI Tools to:

- Draft general communications that contain no client information
- Summarize publicly available documents (news, regulations, grant guidance)
- Generate templates, outlines, or first drafts for staff review
- Brainstorm program ideas, training materials, or board content
- Translate publicly available material into other languages
- Improve the grammar or clarity of staff-written internal documents
- Generate quiz questions, role-play scenarios, or training content

Even with Approved Enterprise AI Tools, the staff member is responsible for reviewing every output before it leaves the organization. AI tools generate plausible-sounding but incorrect information. Treat every output as a draft from a confident intern, not a finished product.

5. Prohibited Uses

The following uses are not permitted under any circumstances:

5.1 — Never enter client information into a Public AI Tool

This includes names, dates of birth, Social Security numbers, Medicare numbers, addresses, phone numbers, medication lists, case notes, intake forms, photos of IDs, or any combination of details that could identify a specific client. This applies even if the staff member believes they are anonymizing the information.

5.2 — Never use AI to make eligibility, benefits, or care decisions

AI tools may not be used as the sole basis for decisions about whether a client qualifies for services, what level of care they receive, or how benefits are calculated. AI may inform staff thinking, but a qualified human must make and document the final decision.

5.3 — Never use AI to generate communications that impersonate clients or staff

AI-generated voices, photos, or written content may not be used to represent that something was said or done by a specific person without that person's explicit, written consent.

5.4 — Never use AI to bypass legal review

AI-generated contracts, releases, consent forms, HR policies, or compliance documents must be reviewed by qualified legal counsel before use. AI may help draft, but it does not provide legal advice and does not replace counsel.

5.5 — Never share AI output as your own work product when authorship matters

In grant applications, board materials, fundraising appeals, and other contexts where authorship is implied or required, staff must disclose substantive AI assistance per funder and donor requirements.

6. Data Handling Requirements

6.1 — The Data Inventory

Staff using AI tools must understand what category of data they are working with. The organization maintains a data classification list at [LINK / LOCATION]. When in doubt, ask the [PRIVACY OFFICER / DESIGNATED ROLE] before entering anything into an AI tool.

6.2 — Prompt Hygiene

Before pasting any text into an AI tool, the staff member is responsible for removing:

- All names of clients, family members, and other identifying individuals
- All addresses, phone numbers, email addresses, and account numbers
- All medical record numbers, Medicare/Medicaid identifiers, and SSNs
- All combinations of detail that could identify a specific person even without a name (e.g. 'the 82-year-old widow on Maple Street with the recent hip surgery')

6.3 — Output Review

Every AI output that will be used externally — sent to a client, submitted to a funder, posted publicly, used in a presentation — must be reviewed by the responsible staff member for accuracy, appropriateness, and any AI-generated errors before use.

6.4 — Audit and Logs

[ORGANIZATION NAME] retains audit logs of approved enterprise AI tool usage for [RETENTION PERIOD — TYPICALLY 90 DAYS] for incident investigation and policy compliance. Staff should assume that AI usage is reviewable by management and have no expectation of privacy in their AI tool prompts when conducting organization business.

centrexIT

7. Training

All staff with access to client information must complete AI safety training:

1. At onboarding, before being granted access to organization systems
2. Annually thereafter, in conjunction with general data security training
3. Within [30 DAYS] of any material change to this policy

Training records are maintained by the [HR / PRIVACY OFFICER / DESIGNATED ROLE].

8. Incident Reporting

Any of the following must be reported immediately to the [PRIVACY OFFICER / EXECUTIVE DIRECTOR]:

- Suspected exposure of client information to a public AI tool
- Suspected AI-generated impersonation of staff, clients, or the organization
- Discovery of a colleague using AI tools in a way that violates this policy
- AI output that may have been relied on for a decision and turned out to be incorrect
- Any incident involving deepfake voice, video, or photo content

Reports may be made in good faith without fear of retaliation. The organization will investigate, take appropriate corrective action, and notify affected clients, funders, and regulators as required by law.

9. Enforcement

Violations of this policy may result in retraining, suspension of AI tool access, formal discipline, or termination, depending on the nature and severity of the violation. Volunteers and contractors are subject to dismissal from their role with the organization.

Repeated or willful violations involving client information will be referred to the appropriate licensing board, funder, and law enforcement as required.

10. Policy Review

This policy is reviewed by [DESIGNATED COMMITTEE / EXECUTIVE LEADERSHIP] at least annually and updated as AI tools, regulations, and best practices evolve. The current version date is recorded in the footer of this document.

ACKNOWLEDGMENT

I have read and understand the Staff AI Acceptable Use Policy. I agree to comply with this policy in all activities I conduct on behalf of [ORGANIZATION NAME]. I understand that violations may result in discipline up to and including termination of my role with the organization.

Name: _____ Date: _____

centrexIT™

Signature: _____

WANT A SCORE INSTEAD?

The Elder AI Risk Snapshot is a free 2-minute self-assessment that scores your AI risk across data governance, staff use, and client vulnerability — and tells you which of the items above to prioritize.

Go to **centrexit.com/tools/elder-ai-risk-snapshot**

YOU CALL. WE ANSWER. IT WORKS