

ARTIFICIAL INTELLIGENCE (AI) ACCEPTABLE USE POLICY

REFERENCE

- U.S. Department of Labor Training and Employment Guidance Letter (TEGL) 03-25 — WIOA Sections 101 and 107, AI literacy funding authority
- U.S. Department of Labor Training and Employment Notice (TEN) 07-25 — AI Literacy Framework
- 2 CFR 200.79, Personally Identifiable Information; 2 CFR 200.82, Protected Personally Identifiable Information
- Code of Virginia § 2.2-3803; § 18.2-186.6
- AARWC Confidentiality & Guidance on the Handling and Protection of Personally Identifiable Information (PII) Policy
- Arlington County DTS AI Acceptable Use Policy; City of Alexandria IT Department AI Acceptable Use Policy
- AARWC SOP 2026-01A: WIOA Case Documentation Agent in Microsoft Copilot — issued separately

DEFINITIONS

- Artificial intelligence (AI): Machine-based systems that, for a given set of human-defined objectives, generate predictions, recommendations, or decisions influencing real or virtual environments by processing data and inputs.
- Generative AI: A subset of AI capable of producing new text, images, spreadsheets, audio, video, or code in response to user prompts.
- Approved AI tool: A platform, license, or embedded AI feature — including Copilot Agents — that has been reviewed and approved by the employing jurisdiction's IT authority (Arlington County DTS or City of Alexandria IT, as applicable) and logged in to that jurisdiction's official AI Register.
- Public or consumer AI tool: A free or consumer-grade generative AI platform — standard ChatGPT, free Gemini, unapproved browser extensions — lacking an enterprise data-protection agreement. Public and consumer AI tools may never be used for any work involving PII and/or PHI.
- Jurisdiction AI Register: The official AI system register maintained by Arlington County DTS or the City of Alexandria IT Department, which is the authoritative record of approved, restricted, and reviewed AI tools for staff employed by or assigned through that jurisdiction. The AARWC does not maintain a separate AI register; approval and registration authority rests with the jurisdictions.
- Restricted use: Any AI application involving sensitive information, a critical business function performed without human oversight, automation coding deployed in production, or system integration with a jurisdiction or partner-agency system. Any new restricted use — including a new custom Copilot Agent or a new third-party AI tool — must go through the AARWC Local System Administrator and the applicable jurisdiction's IT authority before use.
- Local System Administrator: The AARWC staff member designated as the point of contact for AI tool and Copilot Agent requests, responsible for routing requests through internal AARWC director approval and then to the applicable jurisdiction's IT authority for review and registration.

POLICY

This policy sets the conditions under which artificial intelligence tools may be used by WIOA staff. It defines which tools are approved, how new tools and agents are requested and registered, what may and may not be done with participant information, and what happens when the rules are not followed.

This policy supplements, and does not override, the AI acceptable-use policy of a staff member's employing jurisdiction — Arlington County Department of Technology Services (DTS) or the City of Alexandria IT Department. Where a jurisdictional policy is more restrictive, the jurisdictional policy governs.

General use

WIOA staff are prohibited from procuring, downloading, or using any AI software, plug-in, browser extension, or custom Copilot Agent for work purposes without prior approval routed through the Local System Administrator. Staff must access approved AI tools only with official agency-issued enterprise credentials. Personal accounts may not be used to conduct any WIOA business.

Approval process for new tools and agents

Microsoft 365 Copilot, Copilot Premium, the AARWC-developed agents (Case Documentation Agent, Policy Assistant, LMI Assistant), and the Microsoft and jurisdiction pre-approved default agents included in the enterprise tenant are currently approved for use, including advanced or PII-adjacent workflows consistent with this policy's data rules.

Any WIOA staff member who wants to use a different third-party AI tool, wants a new custom Copilot Agent built, or wants an existing AARWC-developed agent expanded must complete the following steps before any use begins.

1. Staff request: The staff member submits the request to the Local System Administrator, describing the intended task, the tool, and any data involved.
2. Executive Director approval: The Local System Administrator obtains approval from the AARWC Executive Director before proceeding.
3. Jurisdictional IT review: The Local System Administrator submits the approved request to the applicable jurisdiction's IT authority — Arlington County DTS or City of Alexandria IT — for security, privacy, and Register review.
4. Registration and authorization: The tool or agent may be used only after the jurisdiction's IT authority approves it and logs it into the Jurisdiction's AI Register. The Local System Administrator communicates the approval and any use conditions to staff.

No staff member may bypass this process, and no AI tool or custom agent may be used for a restricted-use function until steps 1 through 4 are complete.

Acceptable use cases

Approved AI tools may be used for the functions below, provided every requirement in the PII and data restriction rule is followed.

Low-risk general administrative tasks

- Improving the readability, grammar, and formatting of draft reports or internal memos.
- Translating general outreach materials into community languages, provided no client information is included.
- Drafting meeting agendas, training outlines, and outreach templates.
- Summarizing lengthy, publicly available federal regulations, TEGLs, or labor market reports.

Case management and participant support using approved tools only

- Drafting structured case notes using the Case Documentation Agent, from de-identified caseworker input.

- Supporting goal planning and Individual Employment Plan (IEP) drafting using de-identified participant scenarios — barriers, career interests, training goals — with no names, case numbers, or other identifiers included.
- Generating draft career pathway or training-option summaries for a caseworker to review and personalize before sharing with a participant.

Low-risk labor market and research support

- Researching and summarizing labor market information, industry trends, and in-demand occupations using the LMI Assistant, Researcher, Analyst, or other approved tools.
- Drafting employer outreach materials, business services talking points, or sector strategy summaries using publicly available data.
- Comparing training provider or credential information from public sources to support ETPL-related research.

AI-produced work shared internally or externally must be attributed as such. Case managers remain fully accountable for reviewing, correcting, and approving all AI-assisted output before it is shared with anyone.

Prohibited AI use cases

AI tools shall never be used to:

- Determine an individual's program eligibility, suitability for services, training approval, or performance rating.
- Formulate or justify hiring, disciplinary, promotion, or termination decisions.
- Generate legal interpretations, contractual commitments, or grant compliance determinations without qualified managerial and legal review.
- Store, type, or manage system passwords, access codes, or network credentials.

PII, PHI, and data restriction rule

No personally identifiable information (PII) or personal health information (PHI), as defined in the Council's Confidentiality & PII Policy, may be entered, uploaded, or discussed in any AI tool — including approved tools — except as expressly permitted under the recording, transcription, and consent section below, or through the Case Documentation Agent's secure workflow described in its standard operating procedure.

Resumes, case-closure summaries, individual employment plans, and barrier evaluations must never be uploaded unscrubbed. All identifiers — names, addresses, Social Security numbers, dates of birth, and specific employer or school names — must be scrubbed from the document before entry into an AI tool, unless the interaction is a jurisdiction-approved, consented recording as described below. Additionally, scenario-based questions must use fully de-identified language: "a dislocated worker from the technology sector," not a named individual and employer.

AI vendors must contractually certify, through each jurisdiction's procurement and IT review process, that data, staff prompts, and participant uploads will never be used to train or refine proprietary models.

Recording, transcription, and consent

Any AI feature that records or transcribes a meeting or session — for example Microsoft Teams Copilot — is subject to jurisdictional IT approval before use. Two categories apply:

- I. Prohibited without exception: AI recording or transcription is never permitted for:
 - HR disputes, performance evaluations, or disciplinary discussions.
 - Executive session, procurement, or contract negotiation discussions.
 - Any session where a participant has not provided consent.

2. Permitted with documented client consent and approved tools: WIOA intake sessions, eligibility interviews, and case-management interviews involving PII or PHI may be recorded or transcribed using an approved enterprise AI tool only when all of the following conditions are met:
 - Consent: The client has been informed, before the session starts, that the meeting will be transcribed by an AI assistant; has had the purpose of the transcript explained; and has given documented consent, verbal and on the record, to proceed. The client must be offered the option to decline with no impact to their eligibility or services, in which case the caseworker reverts to manual notetaking.
 - Approved tool only: Only an enterprise-licensed, jurisdiction-approved AI tool may be used. Consumer-grade or unapproved transcription tools, ex. free Otter.ai, Fireflies.ai, unvetted browser extensions, etc., remain strictly prohibited, with no exception.
 - Access and retention: The resulting transcript is a confidential case record subject to the Council's Confidentiality & PII Policy, stored only within the secure case file or an access-restricted enterprise location, and retained or purged according to the applicable records retention schedule. The transcript may not be forwarded, copied, or referenced outside the official case file.
 - No model training: The transcript and any PII it contains must never be used by the AI vendor to train, refine, or update a model.
 - Human accountability: WIOA staff remains responsible for reviewing the transcript or any AI-generated summary for accuracy before it is relied upon or entered into the case management system. The AI output does not replace the caseworker's own case note.

For all permitted recordings, consented case sessions and general operational meetings alike, WIOA staff must provide advance written notice of AI use and read a verbal consent script at the start of the meeting, offering an immediate opt-out with no penalty to objecting participants. Participants must verbally reconfirm their consent after the consent script is read by the WIOA staff.

Governance and escalation

The AARWC Executive Director, supported by the Local System Administrator, is responsible for receiving staff requests for new AI tools or custom Copilot Agents, approving them internally, and submitting them to the applicable jurisdiction's IT authority for review and registration. The AARWC does not independently approve or register restricted-use tools; final authority rests with Arlington County DTS or City of Alexandria IT, consistent with each jurisdiction's own AI governance policy.

Existing approved tools

Microsoft 365 Copilot and Copilot Premium; the AARWC-developed Case Documentation Agent, Policy Assistant, and LMI Assistant; and the Microsoft and jurisdiction pre-approved default agents included in the Copilot Premium tenant have already completed jurisdictional review and remain approved for continued use under the conditions of this policy. No re-approval is required for these tools solely because this policy has been adopted. Any expansion of an AARWC-developed agent's system access, data source, or core function requires a new request through the approval process above. Changes to the pre-built Microsoft and jurisdiction agents are governed by Microsoft's and the jurisdiction's own update and review cycles, not by an AARWC-initiated process.

This policy will be reviewed annually by the AARWC Executive Director and the Local System Administrator to reflect changes in jurisdictional IT policy, USDOL guidance, or approved tools.

Training

All WIOA staff must complete AI security and literacy training as a condition of receiving AI tool access. Training must be completed within 30 days of initial notice. AI tool access may not be granted or continued beyond that 30-day window without completed training.

Violations and enforcement

Uploading PII and/or PHI into an unapproved AI tool, bypassing the approval process for new tools or agents, recording a meeting without consent, or using a non-approved public or consumer AI tool for WIOA business will result in the following corrective action:

- First time: Written warning and mandatory retraining.
- Second time: Suspension of AI platform access and formal HR review.

Depending on the severity of the violation, and/or a repeated violation, disciplinary action will be considered.