



Policy and Procedure

TITLE OF POLICY: AI Usage	ORIGINAL EFFECTIVE DATE: 08/01/2025
ICL POLICY #: GOV-007	DATES OF REVIEW/REVISIONS:
DEPARTMENT/PROGRAM: Admin	
<i>This policy will be reviewed every year or upon external or internal stakeholder needs, requirements, or mandates.</i>	
DOCUMENT CONTROL ADMINISTRATOR SIGNATURE:	
Signed by:  3ADB22C97C9B498...	
DATE:	
SPONSORING EXECUTIVE SIGNATURE:	
Signed by:  8B9D034A0FA6432...	
DATE:	

1. Definitions

Term	Definition

2. Purpose

Define the purpose of what the department is trying to achieve. How does this policy meet the needs of ICL, our clients, or statutory/regulatory controls?

To promote the efficient and ethical use of Artificial Intelligence (“AI”) tools, while minimizing the risk of intentional or unintentional misuse that may result in harm.

3. Policy

Define what you are putting in place to achieve your defined purpose. This should be a narrative of what the policy is. What are the guidelines/actions the department wants to achieve?

ICL permits staff to use AI to automate the ordinary and innovate the extraordinary (e.g., improve productivity, enhance service delivery, etc.). The agency considers AI usage an extension of employee work, and not a loophole. Whether embedded in other software, a standalone system, a chatbot, large language model, internally or externally developed, or otherwise, staff may only use agency-approved AI tools for legitimate agency purposes. Staff are accountable for the quality of their AI-supported work. As such, staff are required to review and edit all AI-generated output for accuracy, tone, and alignment with agency objectives and that final content reflects human judgement before using or sharing it. Staff are to exercise due diligence and critical thinking whenever using AI-generated outputs, as AI may produce biased, inaccurate, or inappropriate results. Should an approved AI tool produce an unexpected or unintended result, staff must promptly report it to appropriate personnel for review and corrective action. Use of AI must comply with all applicable laws, regulations, and ethical standards, including but not limited to privacy, data protection, intellectual property, and non-discrimination laws. Employees are expressly prohibited from uploading or transmitting any data that is confidential, proprietary, or protected by regulation (e.g., personally identifiable information of clients, staff, partners, or other stakeholders). All agency AI processes begin and end with a person. Whenever possible, the agency strives to implement AI tools that are transparent, explainable, and capable of providing clear insights into how decisions are made.

4. Procedure

This section should be set out in bullet points. What are the steps the department will perform to ensure the above policy is met with specific guidelines and actions? Include specific roles and responsibilities of associated staff.

1. Evaluation of AI Tools

- a) The IT Department will be vested with sole authority to evaluate AI tools for potential use by staff based, among other factors, upon their utility and security;
- b) Whenever evaluating an AI tool, the IT Department will leverage the AI Tool Vetting Checklist attached as "Appendix A" and, at a minimum, review the following:
 - The tool's security features, terms of service, and privacy policy;
 - The reputation of the AI tool developer and any third-party services used by the tool;
 - Risk in relation to staff only using the tool for its intended purpose, in accordance with any applicable laws and regulations, and in a manner consistent with ICL's mission, vision, and values;
 - *If possible/practical*, the degree to which staff will be able to exercise due diligence and critical thinking when using the outputs the tool generates (i.e., detect biased, inaccurate, or inappropriate results) and ensure their alignment with organizational goals; and
 - The degree to which staff final work products, even when assisted by the tool, will be able to maintain a human touch and reflect employees' own expertise and judgement (i.e., person-centered care, respect for client dignity/independence, etc.).

2. Permitted Usage

- a) Staff will only use AI tools that have been approved by the IT Department;
- b) Approved AI tools will only be used in a manner that enhances productivity, supports change, and/or helps achieve the agency's goals;
- c) Subject to Section "2.d)" below, staff will only use approved AI tools for the following purposes:
 - Summarizing publicly available information (e.g., news articles, research papers, industry reports, etc.);
 - Translating public documents or general text for informal use (i.e., a translator must be used for translating official agency documents/templates);
 - Proofreading and grammar checking of non-proprietary and non-sensitive documents;
 - Practicing presentation skills with AI feedback;
 - Learning new industry best practices, programming concepts, or techniques using generic examples;
 - Analyzing public data sets or case studies;
 - Organizing and structuring general workflow processes;
 - Generating generic templates; and
 - Brainstorming general problem-solving approaches;
- d) Staff wishing to use an approved AI tool for a purpose not expressly set forth herein must first inform the Compliance/QA Department, in writing, how the approved AI tool will be used. The Compliance/QA Department in a collaboration with the Executive Team, as necessary, will approve or deny requests within seven (7) days.

3. Prohibited Usage

- a) Staff will not use AI in a manner that:
 - Creates inappropriate, discriminatory, or otherwise harmful content (towards any individual or the agency); or
 - Is contrary to applicable laws/rules/regulations, agency policies/procedures, or the concerns/restrictions of external partners;
- b) Under no circumstance will staff use AI for the following purposes:

Prohibited Purpose	Description
Assessment of Job Applications, Disability-Related Matters, and Employee Performance	AI is expressly prohibited for use in evaluating job applications, assessments for reasonable accommodation, disability-related inquiries, or in the performance assessment of employees.
Financial Analysis and Advisory Activities	Employees are strictly forbidden from employing AI for financial decision-making or issuing financial recommendations, particularly concerning external entities/funders and clients/stakeholders.

Healthcare Diagnosis and Advice	Employees are strictly forbidden from employing AI for assessing individual clients and providing recommendations to individual clients related to that client's healthcare needs. Staff must always direct healthcare-related questions to appropriately licensed/certified clinicians. For healthcare-related policy recommendations, staff must consult the Chief Medical Officer.
Legal Analysis and Consultation	Utilizing AI for legal evaluations or to dispense legal advice is strictly forbidden. All legal advice and evaluations must be sourced from the agency's outside counsel, preferably coordinated through the Compliance/QA Department.

4. Accountability and Transparency

a) Staff will bear direct/personal responsibility for:

- Reviewing, revising, and personalizing any AI-generated content before final use for work purposes;
- The quality and accuracy of all AI-supported work they generate or share; and
- Obtaining and abiding by any AI use restrictions/expectations from external partners and potential partners (e.g., grants, funding applications, etc.);

b) If multiple reliable sources cannot verify "factual" information generated by AI, that information will not be used by staff;

c) Staff will not give access (i.e., login credentials) to any AI tools approved for ICL use to anyone outside the agency without prior approval from the IT Department;

d) Staff will apply the same security best practices the agency uses for non-AI technology purposes (e.g., strong passwords, keeping software up-to-date, following data retention and disposal policies, opting-out of optional data collection when possible etc.);

e) When requested by their supervisor, the Human Resources Department, or the Compliance/QA Department, staff will disclose whether they used AI in specific internal or external communications;

f) The Communications Department will clearly mark public-facing materials that were developed with generative AI capabilities of substantial interpretative AI capabilities in the final product (i.e., AI meaningfully affects the content, tone, or analysis enough that it could impact someone's interpretation, response, or decision-making) with a distinct signifier indicating the use of AI technology;

g) The Compliance/QA Department and the Communications Department will ensure that this policy and other internal guidelines on AI are published (i.e., posted on the ICL website or otherwise made accessible to the public) to promote understanding of the agency's commitment to responsible AI use; and

h) The agency will:

- Continually engage with community members to ensure its use of AI meets the needs and values of clients; and

- Maintain feedback mechanisms (e.g., surveys, Compliance hotline, stakeholder groups, complaint/grievance processes) for stakeholders to report AI-related concerns.

5. Identifying/Mitigating Bias in, and Ensuring Accuracy/Appropriateness of, AI-Generated Outputs

- a) *In the CIO's discretion based upon then-existing capacity* (e.g., resources, abilities, tools, priorities, etc.), the IT Department, in collaboration with the SVP – Quality Improvement and Impact, will:
- Remain aware of common biases that may be present in AI tools (e.g., data bias, algorithmic bias, and confirmation bias);
 - Regularly review and evaluate AI-generated outputs for potential biases and inaccuracies, seeking input from diverse perspectives;
 - Reject AI tools without transparent methodologies and documentation that allows for understanding their decision-making processes;
 - Collaborate with AI vendors and developers to improve AI systems and address identified biases, reporting any issues and working together to develop solutions; and
 - Document and communicate any identified biases and mitigation efforts to staff;
- b) To ensure that AI-generated outputs are accurate and appropriate, staff will:
- Verify the accuracy of AI-generated outputs by cross-checking with reliable sources, human judgment, or other relevant methods;
 - Review AI-generated outputs for appropriateness, taking into account the context, audience, and potential impact of the content;
 - Establish a system of checks and balances involving multiple reviewers to minimize the risk of errors or inappropriate content;
 - Ensure that AI-generated content is properly reviewed and approved by a human before it is published or used for decision-making; and
 - Develop and implement guidelines for the responsible use of AI-generated outputs in different contexts and situations, tailored to the specific needs and requirements of their teams.

6. Ethical and Legal Use of AI Regarding Intellectual Property

- a) Whenever using AI, staff will honor intellectual property rights, including copyright and trademark protections for authors and visual artists (i.e., staff will not use AI to process or share protected, private, or copyrighted material); and
- b) In furtherance of the above, staff will:
- Ensure that AI tools are used in a manner that respects copyright laws and ethical standards;
 - Obtain necessary permissions or licenses before utilizing copyrighted materials;
 - Provide proper attribution to authors and artists when using or sharing their work; and
 - Establish a process for reporting and addressing copyright infringements, including a designated point of contact for reporting such issues.

7. Data Protection and Privacy

- a) Whenever using AI, staff will adhere to separate policy on HIPAA privacy and security including:

- Ensuring that client data is anonymized, encrypted, or otherwise protected when used with AI tools;
- Obtaining appropriate consent from clients, when necessary; and
- Reporting any data breaches or incidents involving AI to the Compliance/QA Department.

- b) NO PROTECTED HEALTH INFORMATION (“PHI”) OR PERSONALLY IDENTIFIABLE INFORMATION (“PII”) ABOUT CLIENTS, STAFF, OR CONTRACTORS WILL BE SUBMITTED TO OR REFERENCED IN AI TOOLS. This includes but is not limited to, names, home addresses, email addresses, social security numbers, telephone numbers, dates of birth, credit card numbers, employment details, educational backgrounds, immigration status, log-in credentials, license plates, faces and voices, audio, photos, and video; and
- c) No proprietary company information, including trade secrets, sensitive internal language, or data containing the company name, or intellectual property, will be submitted, copied, or referenced in any way when interacting with AI tools.

8. Development and Engagement

- a) To the extent the agency, whether through the IT Department, the Quality Improvement and Impact Department, or otherwise, develops AI tools or engages with external collaborators, the following guidelines will be adhered to:

- Safety, privacy, and ethical considerations will be prioritized;
- The development process will include measures to address potential biases (e.g., conducting regular bias audits, seeking diverse input, using fair and unbiased data for model training, etc.);
- All external collaborators will commit to upholding the principles of transparency, accountability, and respect for privacy as outlined in this policy and any other applicable policies or guidelines of the agency; and
- Collaboration agreements will be in writing and clearly define the roles, responsibilities, and expectations of all parties involved as well as ownership and usage rights of AI models and data;

- b) Prior to deployment:

- AI tools will undergo rigorous testing to ensure their safety, accuracy, and reliability (results of testing such testing will be documented); and
- A plan for ongoing monitoring and maintenance will be developed/implemented to ensure that the tools continue to operate safely and effectively, and that any new issues or concerns are promptly addressed;

- c) Any potential risks or ethical concerns related to the AI development or collaboration will be reported to the Chief Compliance and Privacy Officer.

9. Use of AI Meeting Notetakers

- a) AI meeting notetakers (i.e., tools that have been approved by the IT Department to automate the process of capturing, transcribing, and summarizing meeting discussions) will only be used for meetings exclusively attended by employees (e.g., no clients, non-staff members, etc.);

- b) Whenever using AI meeting notetakers to facilitate accurate documentation and sharing of meeting discussions, staff will:
 - Obtain necessary permissions from meeting participants;
 - Ensure the accuracy of AI-generated notes by reviewing and, if necessary, editing the content; and
 - Abide by data privacy standards, ensuring that sensitive information is properly handled and stored;
- c) Meeting participants will be provided an option to opt-out if desired. In such a situation (i.e., if a meeting attendee explicitly opts-out of AI notetaking), the meeting facilitator/host will respect the decision of the attendee by:
 - Disabling the AI notetaker for the specific attendee or for the entire meeting, if necessary; or
 - Excusing the attendee from the meeting.

10. Human Verification and Review

- a) Staff will not use AI as a substitute for human judgment and decision-making; and
- b) No final staff decisions and/or determinations will be made by AI, and any information, fact, or figure created by AI and used in ICL public facing materials (or that inform decisions and/or determinations) will be independently reviewed and verified by a member of the Communications Department.

5. References/Citations

Indicate any relevant references or citations (include statutory/regulatory numbers and accreditation standards).

6. Training Requirements

If applicable, what training requirements are mandated by ICL and/or oversight agencies?

1. The agency will continually assess the need for AI training among staff as AI capabilities evolve. *In the discretion of the Human Resources Department*, staff training may encompass the Workforce Development Department (during new employee orientation (“NEO”), annual refreshers thereafter, and/or otherwise) providing information on the responsible and ethical use of AI that including guidelines for:
 - a) Handling client information in compliance with HIPAA regulations;
 - b) Identifying and reporting potential security incidents, breaches, or unauthorized disclosures;
 - c) Familiarizing themselves with this policy and any other relevant policies, guidelines, and best practices; Presentation of the Dos and Don’ts attached as “Appendix B”; and/or
 - d) Learners having to execute the AI Usage Attestation attached as “Appendix C”.

- 2. Specific staff (e.g., CIO, SVP – Quality Improvement and Impact, the Chief Compliance and Privacy Officer, etc.) will attend external training sessions and/or workshops to stay updated on AI-related developments, risks, and mitigation strategies.

7. Monitoring

What departmental meetings, reports, inspections, audits, or other activities will ICL conduct to ensure this policy and procedure is followed by the organization?

- 1. All staff interactions and activities with AI tools will be logged and monitored for security and compliance purposes. Audit logs will be retained for such time periods defined by separate data retention policies.
- 2. The IT Department will run periodic reports intended to verify that:
 - a) Only approved AI tools are being used by staff;
 - b) All approved AI tools are performing as intended (i.e., their validity, accuracy, robustness, and reliability contribute to trustworthiness and unanticipated failures are not causing harm); and
 - c) Vendors security protocols are sufficient.
- 3. Staff will be transparent about their own use of AI. This includes:
 - a) Disclosing the use of AI tools when communicating with external stakeholders (e.g., clients, donors, partners, etc.); and
 - b) Maintaining a record of AI tool usage, including the purpose, inputs, outputs, and any actions taken based on the AI-generated results.
- 4. Intentional *and* unintentional misuse of AI and/or other violation of this policy may result in disciplinary action, up to and including termination of employment, in accordance with the agency’s procedures for progressive discipline. For purposes of the foregoing:

Misuse Type	Description	Examples
Intentional	Any intentionally malicious activity that violates ethical, legal or moral standards, and compromises the safety, privacy, or security of individuals or society as a whole. Intentional misuse of AI systems is expressly forbidden.	▪ AI-based fraud (i.e., manipulating or cheating unsuspecting individuals or organizations through phishing scams, identity theft, or fraudulent behavior); ▪ Discrimination (i.e., perpetuating discrimination, resulting in either unequal treatment or exacerbation of existing social inequalities); ▪ Invasion of privacy (i.e., exposing non-anonymized/non-encrypted client information or the use of AI to gather personal data without the consent of individuals, leading to the violation of privacy right); ▪ Malicious use (e.g., cyber-attacks, phishing attempts, social engineering, vulnerability identification and exploitation, etc.); and

		▪ Spreading misinformation (i.e., creating and/or distributing false or misleading information).
Unintentional	Situations where staff, without malicious intent, use AI tools in ways that lead to negative consequences or harm. This can occur due to a lack of understanding, insufficient training, or an oversight in the use of AI technology.	▪ Bias (i.e., unawareness of the potential biases embedded in AI algorithms or training data); ▪ Inaccurate information (i.e., unknowingly relying on AI-generated outputs that are incorrect/outdated); and ▪ Overreliance (i.e., relying too heavily on AI tools, neglecting to apply one's own judgment, expertise, or common sense).

5. Staff will be encouraged to report any suspected misuse of AI systems, *whether intentional or unintentional*, to their supervisor or other appropriate person(s) (e.g., the Compliance/QA Department). Reports received through the Compliance Hotline will be processed anonymously and handled confidentially. As warranted/required by applicable regulations, reports will result in containment efforts, investigation, mitigation, and/or notification of affected individuals.
6. STAFF ARE EXPRESSLY PROHIBITED FROM USING UNAPPROVED AI TOOLS FOR WORK PURPOSES AND FROM USING ANY AI TOOLS WHILE AT WORK FOR NON-WORK PURPOSES.

8. Appendices

Include any additional pertinent information/material needed.

Appendix A – AI Tool Vetting Checklist

Appendix B – AI Do's and Don'ts

Appendix C – AI Usage Attestation

AI Tool Vetting Checklist

1. Purpose & Clinical Relevance

- ☐ Is the AI application appropriate for behavioral health (e.g., care coordination, early intervention, risk prediction)?
- ☐ Does it align with person-centered, trauma-informed, and recovery-oriented principles?
- ☐ Does it enhance access, quality of care, or client outcomes?

2. Data Governance & Privacy

- ☐ Is Protected Health Information (PHI) handled in compliance with HIPAA?
- ☐ Are behavioral health-specific confidentiality rules (e.g., 42 CFR Part 2) addressed?
- ☐ Is informed consent built into AI-enabled processes where applicable?
- ☐ Are data storage, access, and retention policies clearly defined?

3. Clinical Performance & Safety

- ☐ Are clinical validation studies or peer-reviewed results available?
- ☐ Does the tool support—not replace—clinical judgment?
- ☐ Are mechanisms in place to handle uncertainty or escalate care when needed?
- ☐ Has the AI been evaluated for safety, false positives, and unintended consequences?

4. Explainability & Provider Trust

- ☐ Can staff understand how the AI arrives at decisions or predictions?
- ☐ Are model outputs presented in clear, plain language?
- ☐ Can clinicians override AI-driven recommendations?

5. Integration & Workflow Fit

- ☐ Is the solution compatible with Electronic Health Records (e.g., Netsmart)?
- ☐ Can it be used with existing programmatic workflows?
- ☐ Does it reduce staff burden (e.g., documentation, data entry)?
- ☐ Does it integrate with appointment scheduling or care team coordination?

6. Security & Compliance

- ☐ Is the vendor compliant with HIPAA and 42 CFR Part 2?
- ☐ Are there controls against data breaches and cyber threats?
- ☐ Is a Business Associate Agreement (BAA) available and up to date?
- ☐ Is the AI monitored for ongoing regulatory compliance?

7. Human Oversight & Clinical Accountability

- ☐ Are licensed professionals part of decision-making loops?
- ☐ Is there clear guidance for when human intervention is required?
- ☐ Can care managers, clinicians, or peers report concerns or errors?

8. Vendor Credentials & Ethics

- ☐ Is the vendor experienced in behavioral health and government-funded service environments?
- ☐ Are model development practices and datasets transparent?
- ☐ Does the vendor adhere to responsible AI practices and provide support?

9. Impact, Evaluation & Equity Monitoring

- ☐ Are there KPIs to measure success (e.g., reduced hospitalizations, improved access)?
- ☐ Can performance be monitored continuously and adjusted if needed?
- ☐ Are underserved or high-need populations appropriately considered in model application?

10. Quality Management & Outcomes Reporting

- ☐ Does the tool support population health tracking or outcome-based care?
- ☐ Can it contribute to or automate quality reporting (e.g., CARF)?
- ☐ Is data exportable for performance dashboards or quality audits?
- ☐ Can it support persons in services-reported outcomes or satisfaction surveys?

11. Governmental Reporting & Compliance

- ☐ Does the AI facilitate reporting to federal/state entities (e.g., Medicaid)?
- ☐ Is it compatible with funding-specific reporting requirements (e.g., HUD, DOHMH)?
- ☐ Can it support grant performance tracking or deliverable submissions?
- ☐ Are templates or workflows available for compliance reports?

12. Accounting & Revenue Cycle Management

- ☐ Does it support billing workflows (e.g., encounter documentation, claim generation)?
- ☐ Can it help identify billing errors, missed charges, or audit risks?
- ☐ Is it compatible with existing revenue cycle or billing software?
- ☐ Does it improve tracking of accounts receivable, collections, or denials?
- ☐ Can it assist in optimizing payer mix or contract performance?

AI Do's and Don'ts

As we bring AI into our day-to-day work at ICL, it's important to use these tools in a way that helps us do our jobs better while sticking to our values. Here's a simple guide to make the most of AI without running into trouble.

Do's	Don'ts
▪ Use AI to Make Work Easier – Feel free to use approved AI tools for things like writing drafts, summarizing info, or scheduling tasks. Let AI help you brainstorm ideas or handle repetitive stuff like filling in forms. ▪ Double-Check AI's Work – Always take a moment to review and fact-check anything AI suggests before you use it in emails, reports, or decisions. Make sure what AI generates lines up with ICL's mission and values. ▪ Keep Sensitive Info Safe – Be careful about putting sensitive information into AI systems. Only use AI tools that have been approved by IT Department. ▪ Keep the Human Touch – AI is here to help, not take over. Make sure to use your own expertise and judgment when AI suggests something. Always have a human double-check important work before it goes out the door. ▪ Keep Learning – Stay up to date by completing all required AI training sessions and sharing what you've learned with your team. If you discover a cool AI trick, pass it on so everyone can benefit. ▪ Use AI Ethically – Make sure your use of AI is fair and transparent and look for any biases in the AI's outputs. If something doesn't seem right or fair, take the time to adjust it. ▪ Be Transparent – Let people know when you worked with AI to produce something.	▪ Don't Share Private Information – Never put confidential client or staff details into AI tools. ▪ Don't Depend on AI for Everything – AI is a tool, not a decision-maker and not a replacement for humans. Always use your own knowledge to double-check AI's work. ▪ Don't Use Unapproved AI Tools – Only use AI tools that have been approved by the IT Department to keep things safe and secure. ▪ Don't Break Privacy Rules – Make sure everything you do with AI follows privacy laws like HIPAA. Be extra cautious when handling client data to avoid any privacy breaches. ▪ Don't Skip Security Measures – Don't turn off or ignore any security settings on AI tools. If you spot any issues, let the IT Help Desk know right away. ▪ Don't Plagiarize – Make sure the content AI creates is original or properly credited. ▪ Don't Pretend – Be upfront and transparent when AI has played a role in creating something.



AI Usage Attestation

By signing below, I attest as follows:

1. I have read, understood, and agree to abide ICL's AI Usage policy;
2. I am committed to using only agency-approved AI tools and using them only in a responsible, ethical, and legal manner.
3. I acknowledge that AI may be used to enhance my work and not as a substitute for my own judgment and any AI-generated content requires human review and verification.
4. I will not intentionally use AI for malicious or harmful purposes.
5. I will handle AI-related data with care, in accordance with privacy regulations and agency policies. I will not input the sensitive, confidential, or personally identifiable information of clients or staff into a public AI tool (e.g., ChatGPT).
6. I understand potential risks related to data breaches or unauthorized access when using AI and agree to report any concerns, issues, or suspected misuse of AI tools through the appropriate channels.
7. I will participate in all agency-required trainings/workshops intended to enhance AI literacy and/or ensure compliance AI-related guidelines.

Signature

Printed Name: _____

Date: _____