



Module 1: Understanding and Communicating AI in Human Services

1.3: Reviewing Your AI Acceptable Use Policy

New York Alliance for Inclusion & Innovation
AI Community of Practice / Learning Community

2025



Featured Guest:
Gregg Paulk
Chief Information Officer
Anderson Center for Autism





© 2025 New York Alliance for Inclusion & Innovation

This content was developed and is owned by the New York Alliance for Inclusion & Innovation for the exclusive use of its AI Learning Community and Community of Practice.

Artificial intelligence (AI) is rapidly evolving, and best practices may change. Users should regularly verify that this information remains accurate, relevant, and timely for their needs. Each agency is responsible for developing, implementing, training, and enforcing its own AI policies—including compliance with all applicable laws, ethical standards, and protections for protected health information (PHI) and privacy.

Unauthorized reproduction, distribution, or modification is prohibited.





Module 1: Understanding and Communicating AI in Human Services

1. What Is AI (and What Isn't)?

- Introduces artificial intelligence with simple definitions, key distinctions (e.g., generative AI vs. traditional automation), and real-world relevance for human services.
- Explains how large language models (LLMs) like ChatGPT work and why most modern AI tools are built on generative foundations.

2. How to Talk About AI Use

- Provides language, principles, and strategies for transparently disclosing AI use to staff, individuals receiving services, and families.
- Shows how AI is evolving from basic automation to dynamic support systems, with examples from disability services.

3. Reviewing Your AI Acceptable Use Policy

- Covers essential components of an ethical and practical AI use policy, including data protection, approved tools, and human oversight requirements.
- Helps organizations draft or refine policies to align with their mission and regulatory needs.



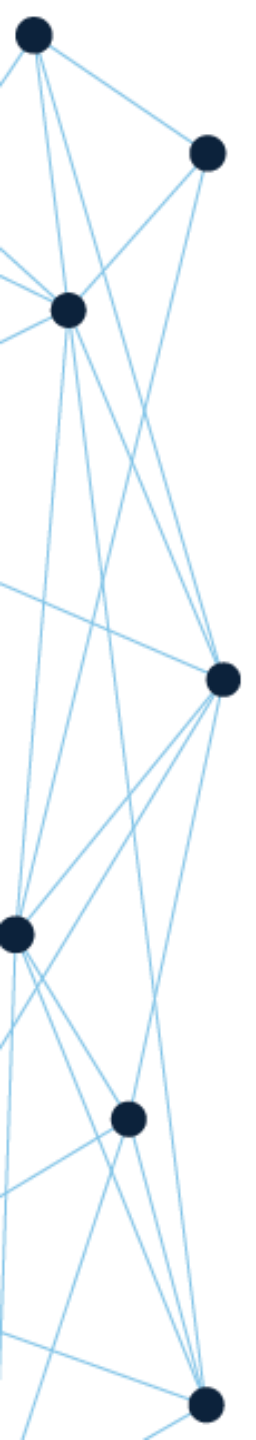


Reviewing Your AI Acceptable Use Policy

- Covers essential components of an ethical and practical AI use policy, including data protection, approved tools, and human oversight requirements.
- Helps organizations draft or refine policies to align with their mission and regulatory needs.



Risks and Concerns



Loss of Human
Judgment

Bias &
Discrimination

Privacy & Data
Exploitation

Job
Displacement &
Staff Distrust

Over-
Dependence

Environmental
Resources

Costs for
Implementation
and Ongoing
Use





New York Alliance 2024-2025 Initial Organizational Self-Assessment Findings

Assesses leadership alignment, planning, and cross-organizational strategy for AI use (n=32).

56.7%

Does your agency have a formal or informal committee or group dedicated to discussing AI strategy and ensuring it aligns with your overall mission and vision?

46.7%

Is AI explicitly mentioned in your agency's current strategic plan?

26.7%

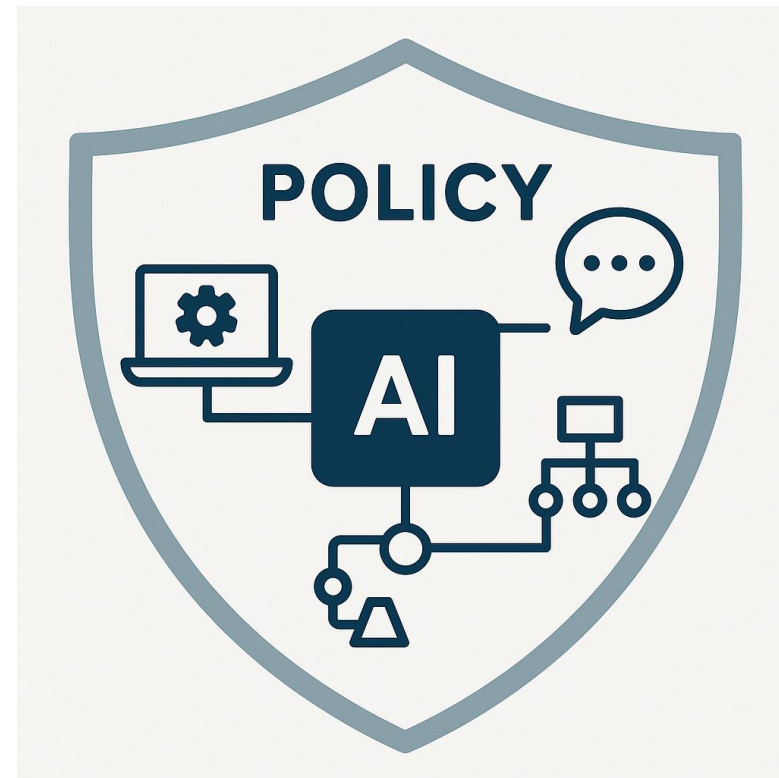
Are there any current policies or procedures within your agency that reference AI use?





Why Your Organization Needs an AI Acceptable Use Policy

- Defines how AI can and cannot be used within your organization.
- Protects data privacy, security, and ethical standards.
- Builds trust among staff, stakeholders, and the people you support.
- While no policy eliminates all risks, having clear guidelines helps manage risks by promoting ethical AI use, protecting privacy, reducing bias, supporting human judgment, and clarifying AI's role to avoid overreliance on AI and reduce staff worries about job impacts.



Acceptable Use Policy Journey Anderson Center for Autism



- Artificial Intelligence Use Agreement
- Computer System / Services Use Agreement
- Standard Operating Procedures: Use and Request of Artificial Intelligence (AI) in Agency Operations

 Anderson Center for Autism LIFELONG LEARNING™	STANDARD OPERATING PROCEDURES	
DEPARTMENT:	HIPAA/HITECH	PROCEDURE: HHC-49
ISSUE DATE:	03.26.2025	PAGE 1 of 3
EFFECTIVE DATE:	04.01.2025	
TITLE:	USE and REQUEST of ARTIFICIAL INTELLIGENCE (AI) in AGENCY OPERATIONS	

Anderson Center for Autism
LIFELONG LEARNING™

Computer System/Services Use Agreement

The purpose of this Agreement is to provide team members, volunteers, contractors and agency associates of Anderson Center for Autism and its affiliates (ACA) with mandated requirements for utilizing ACA computing technologies. This includes all applicable local, State, and Federal laws.

ACA has developed a comprehensive program to ensure the privacy, protection, and security of all electronic information. Standard Operating Procedures (SOPs) are in effect to ensure ACA's compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act of 1974 (FERPA), and the Health Information Technology for Economic and Clinical Health Act (HITECH). All team members, volunteers, contractors and agency associates of ACA (referred to as Workforce Member in HIPAA/HITECH SOPs) are required to comply with all SOPs as outlined in this Agreement.

Use and access to computer systems, services, software and applications will be determined by your specific job descriptions. If you have not been issued a dedicated ACA computer system, check with your supervisor to identify the location of a system for your use. Since ACA utilizes email to promote communications within the agency, you are expected to check your email account at least once per workday during work hours and your Sendio account at least once per week. You are responsible for all equipment issued for your use and you are required to report any malfunction, damage, loss or theft to the IT Department immediately.

A computer system is defined as all equipment and devices, stand-alone, mobile, wireless or networked, which are used for computing, communicating, printing, transferring, or storing data and software applications in digital format. Computer services include, but are not limited to, network server applications and data storage, Internet access, e-mail services, **Cloud Storage, Software As A Service applications (SaaS)** and Outlook email services.

If you are utilizing a portable device to temporarily save or store data, you are required to transfer data files to **secured agency-controlled location** as soon as possible and **delete** from the portable device. All electronic data files must only be saved or stored on an encrypted or secure **agency-controlled location**. You are required to report any malfunction, damage, loss or theft of data to the IT Department immediately.

The content of all computer systems and services remains the property of ACA and will be always monitored by ACA for security and/or network management purposes and agreement compliance. You should have no expectation of privacy. You will be held accountable for any activity associated with your access and use of ACA computer systems. Usage reports reflecting time and websites visited will be monitored.

Workforce members are not permitted to use unauthorized Artificial Intelligence and Large Language Model (AI/LLM) technologies for agency business. For the purposes of this agreement, AI is defined as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. The definition of AI/LLM includes but is not limited to systems that use machine learning, large language models, natural language processing, and computer vision technologies, including generative AI such as, but not limited to, ChatGPT, Bard, Bing Chat, DallE, and LaMDA, etc.

I agree to the following requirements and acknowledge that any deviation or breach must **immediately** be reported to my Supervisor. I agree that I will not:

- Access and use computer systems while actively supervising individuals under my care.
- Allow my password to expire.
- Share my login name(s) and password(s) with anyone.
- Leave the computer without logging out and locking the computer.
- Use computing technologies for any illegal purpose.
- Transmit/receive/access any material that contains illegal, obscene, hateful content that is objectionable and/or inappropriate for the workplace.
- Transmit/receive/access defamatory statements that are intended to annoy, harass, intimidate or threaten another person.
- Use computing technologies for any activity outside of ACA's business mission or operations, including but not limited to social media postings, junk mail transmissions or other advertising schemes.
- Merge personal and ACA email or SMS accounts or transmit ACA information from a personal email account unless specifically authorized to do so.
- Open e-mail attachments or Internet pop-ups which appear suspicious or are from unknown senders which may contain malicious code.
- Use any donated or personal computer systems, hardware or software without the approval of the IT Department.
- Use personal hardware for remote access to ACA networks unless it complies with **industry acceptable** standards and authorization has been issued by the IT Department.
- Connect to any other network while remotely connected to ACA's network.
- Connect any computing **device on-site** or remotely that does not have up to date and enabled anti-malware and antivirus software.
- Remotely access or transmit student/consumer data outside of ACA computer systems without the required encryption of data in compliance with SOP HHC-#17 Acceptable Encryptions.
- Install software or firmware (jailbreak) designed to gain unauthorized access to a device.
- Download any programs onto ACA systems without prior written approval i.e. screen saver, instant messaging or other various programs.
- Upload, download or otherwise transmit confidential data, commercial software or any copyrighted materials belonging to ACA or third parties.
- Access or transmit student/consumer data to any external party unless specifically related to the treatment, payment or operations of the ACA.
- Access or transmit student/consumer data within ACA to any workforce member **that does not** have access rights without Director approval.
- Transmit personal and protected information about individuals outside of ACA computer systems without utilizing **agency approved sharing and/or encryption technology**.
- Take photographs/videos with any computing device without following the requirements of SOP GPS-08.
- Delete or alter any records unless authorized.
- Operate digital devices while operating a motor vehicle.
- Leave digital devices in vehicles unsecured or for extended periods of time.
- Input any personally identifiable information (PII) or Protected Health Information (PHI) into **unauthorized systems including, but not limited to, AI/LLM tools**.

I have read the above and agree to abide by these requirements and understand this Agreement will be maintained in my **Human Resources** file. I understand and acknowledge that any violation or breach of this Agreement may subject me to disciplinary action up to and including termination and possible legal actions.

Team Member Name (Please **print**) _____ Team Member Signature _____ Date (MM/DD/YYYY) _____

S:\Unclassified\AI\Agency Forms\Information Technology\IT-02 Computer System/Services Use Agreement Rev. 2024-03-02 Page 2 of 2

Anderson Center for Autism
LIFELONG LEARNING™

Artificial Intelligence Use Agreement

Purpose:
This agreement outlines the responsibilities and best practices for using AI tools in compliance with privacy and data protection regulations. By signing this agreement, the user acknowledges the importance of not inputting Personally Identifiable Information (PII) or Protected Health Information (PHI) governed by HIPAA into AI systems.

Agreement:
I, the undersigned, understand and acknowledge that:

1. **Compliance with Data Privacy Laws:**
I am responsible for ensuring that the data I use when interacting with AI tools complies with applicable data protection and privacy laws, including, but not limited to, the Health Insurance Portability and Accountability Act (HIPAA) and other relevant regulations governing the use of sensitive data.
2. **Prohibition on the Use of PII and PHI:**
I agree not to input any Personally Identifiable Information (PII) or Protected Health Information (PHI) into AI tools. I understand that AI systems are not designed or approved for processing sensitive personal data unless explicitly authorized by the AI provider with proper data protection mechanisms.
3. **Definitions:**
 - o **AI (Artificial Intelligence)** is a technology that simulates human intelligence with problem-solving capabilities. It can perform tasks that normally require human intelligence. Some common examples are ChatGPT, MS Co-Pilot and Google Gemini etc.
 - o **PII (Personally Identifiable Information)** is any data that can be used to identify an individual. Examples include, but are not limited to:
Full name > Social Security number > Email address
Home address > Telephone number > Date of birth
Financial information (e.g., credit card numbers, bank account information)
 - o **PHI (Protected Health Information)** is any data that relates to an individual's health status, medical history, or healthcare provided, which is protected under HIPAA. Examples include, but are not limited to:
Patient names > medical record numbers > Health insurance information

Consequences of Non-Compliance:
I understand that the unauthorized disclosure of PII or PHI can result in legal penalties, fines, and reputational damage for both the individual and the organization. Violations of this agreement may result in disciplinary actions, including termination of access to AI tools or employment.

Best Practices for Data Protection:
I commit to following best practices when using AI tools, including:
o Anonymizing all data
o Using only de-identified, non-sensitive information for testing, analysis, or processing through AI tools.
o Ensuring that any data I use in AI systems is authorized for such use and adheres to data minimization principles (i.e., only using data that is necessary for the specific purpose).

Data Breach Reporting:
In the event I become aware of a data breach or unauthorized disclosure of PII or PHI, I will immediately report the incident to the Corporate Compliance Department.

By signing this agreement, I acknowledge that I have read, understand, and will comply with the above terms regarding the responsible use of AI tools.

Signature: _____ Name: _____
Date: _____

This agreement ensures the user recognizes the importance of protecting sensitive data when using AI tools, outlining both PII and HIPAA-related information to avoid.

Aligning with Agency AI Policies

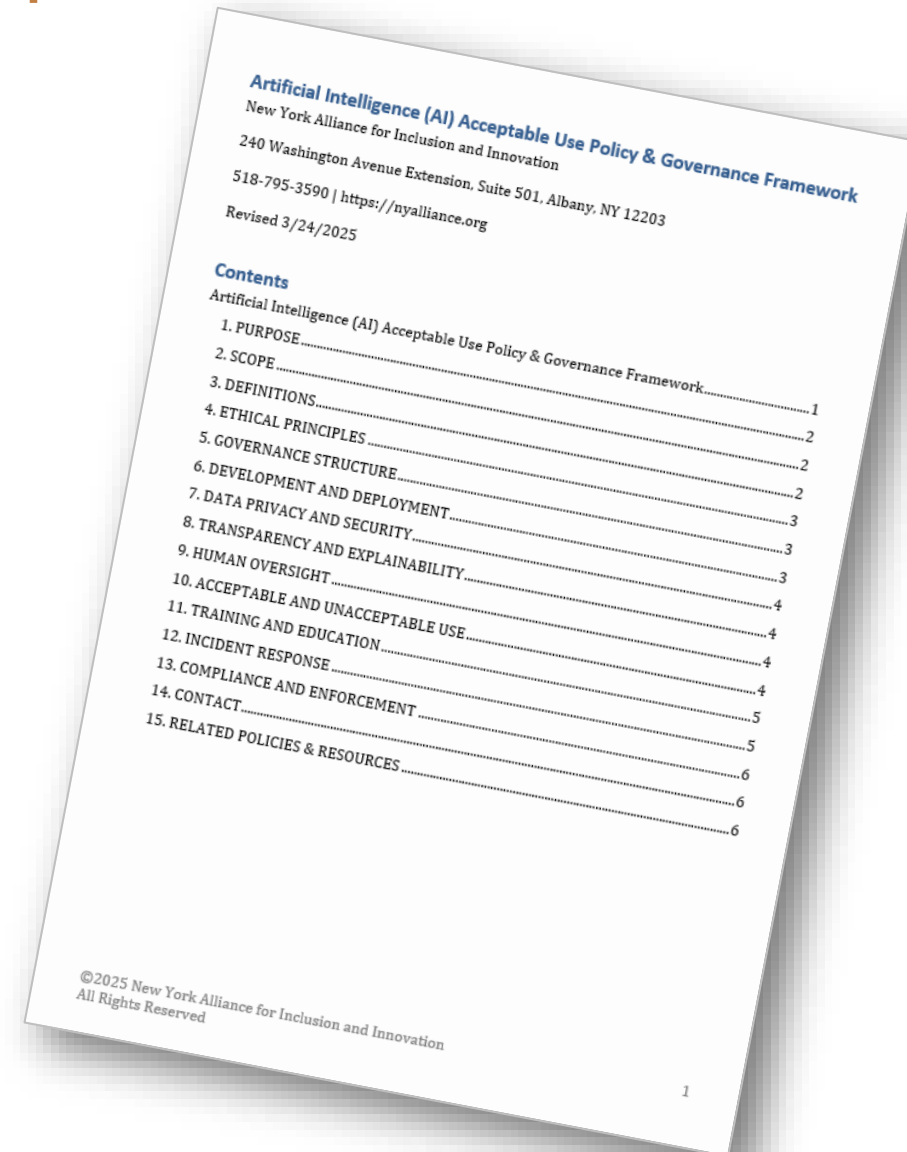
Know Your Policies	Review your agency's Employee Handbook, AI Use Agreement, Computer Systems-Services Use Agreement, and related data security or compliance policies.
Understand Prohibitions	Do not enter confidential or personally identifiable information (PII) / protected health information (PHI) into AI tools unless explicitly approved and secured.
Use Approved Tools Only	Follow agency guidance on which AI tools are authorized and ensure they meet security and encryption standards.
Establish Clear Definitions	Remember that AI includes chatbots, image generators, and other large language models (LLMs).
Know the Consequences	Non-compliance may result in disciplinary action, up to and including termination.
Report Misuse Immediately	Contact your supervisor, Compliance, or IT if you suspect unauthorized AI use or data breach.





Resources Used to Develop These AI AUPs

- **Duke AI Syllabus Policies:** Guidelines for including AI policies in course syllabi
 - <https://lile.duke.edu/ai-and-teaching-at-duke-2/artificial-intelligence-policies-in-syllabi-guidelines-and-considerations/>
- **FERPA Overview:** Student education records privacy protections under federal law
 - <https://studentprivacy.ed.gov/ferpa>
- **HHS HIPAA Administrative Simplification:** U.S. Health and Human Services standards for health data privacy, security, and transactions
 - <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>
- **MIT AI Guidance:** Responsible and effective AI use guidelines for the MIT community
 - <https://ist.mit.edu/ai-guidance>
- **New York State AI Acceptable Use Policy:** State policy on acceptable use of AI technologies (May 2025)
 - <https://its.ny.gov/system/files/documents/2025/05/nys-p24-001-acceptable-use-of-artificial-intelligence-technologies.pdf>
- **NIST AI Risk Management Framework:** U.S. National Institute of Standards and Technology framework for managing AI risks
 - <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>





Review of Sample AI Acceptable Use Policy

Purpose

- Define why your agency is using AI tools (e.g., to support documentation, summarize notes, improve service delivery).

Permitted Uses

- Staff may use approved AI tools **only within secure systems** (i.e. Microsoft Copilot 365 under E3/E5 license).
- Do not use public AI platforms (i.e. ChatGPT in browser) for any data entry involving PHI.

Human Oversight

- AI-generated outputs must always be **reviewed by a human** before use in service plans or communications.

Data Privacy & Security

- Comply with HIPAA, CMS, and NYS policies; no identifiable information should be entered into open/public AI systems.

Staff Responsibilities

- Follow training, report misuse, and stay within role-based access permissions.





Drafting or Refining Your AI Use Policy



Review existing policies for AI relevance.



Identify priority areas needing AI guidelines (i.e., data security, service notes, and service planning tools).



Form an AI oversight committee with cross-functional representation.



Use external resources to strengthen your policy.



Provide training on responsible and approved AI use, data protection, and human oversight (Module 2 of this webinar series).





New York Alliance AI Resource Page

https://nyalliance.org/AI_Toolkit



NY ALLIANCE FOR INCLUSION AND INNOVATION & DATA POTATO

AI Toolkit

TRANSFORMING SUPPORTS & THE WORKFORCE WITH AI

The New York Alliance for Inclusion and Innovation is uniquely positioned to offer templates, toolkits, training, and technical assistance to its membership to help use resources as conservatively and safely as possible while these emerging technologies become commonplace. AI is continuously evolving, as will this toolkit from the New York Alliance. Some of those resources could include:

- Overview webinar and content deck for Artificial Intelligence for Home and Community-Based Providers**
Presenting and reviewing checklists for AI best practices, vendors, security, each with additional detail described in the subsequent resources
- AI Best Practices for HCBS Providers**
Details on ethics, data privacy and security, responsible AI implementation at a provider agency
- Engaging with EHR Vendors**
Understanding the questions to ask, the agreements to have in place with respect to AI, and making sure that the underlying functionality is able to deliver on claims to improve outcomes and workforce efficiencies actually using AI.
- Overcoming AI Challenges**
Practical solutions for technical limitations, security, and organizational readiness.

AI Organizational Self-Assessment

The purpose of this point-in-time OSA is to help provider agencies evaluate their readiness, strengths, and areas for improvement in relation to integrating and managing AI tools and technology within their organization. This assessment covers key areas including technology infrastructure, data security, regulatory compliance, workforce development, and the impact of AI on service delivery quality and outcomes.



Available Now

- AI Organizational Self-Assessment
- Recorded Webinars and Meetings
- Future home for:
 - Policies
 - Training
 - Tools & Templates
 - Community Engagement & Shared Learning





Thank you!

Doug Golub

doug@datapotato.com

cnapierski@nyalliance.org

