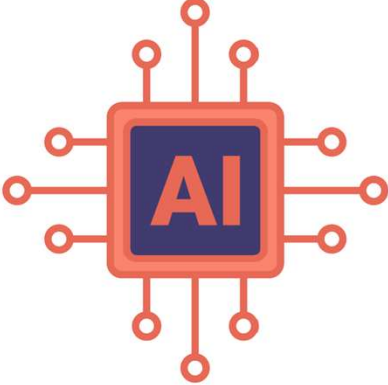




Navigating AI Responsibly

**2026 NECAP
Conference**

October 8, 2026



1



Allison Ma'luf, Esq.
Executive Director/General Counsel
caplawinfo@caplaw.org



2



CAPLAW

**The National Legal
Expert for
Community Action
Agencies**

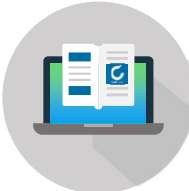
caplaw.org



One-on-One Consultations



In-Person and Virtual Trainings



Online Resource Library

3



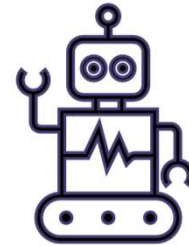
- Artificial Intelligence (AI) Generally
- Legal Framework
 - Potentially Applicable Laws
 - Concerns
 - Tips
- Sample Policy
 - Organizational Approach
 - Key Elements

4

AI Generally

What is it?

- AI technologies are rapidly evolving systems designed to:
 - Approximate human cognition,
 - Act rationally, and
 - Perform tasks without significant human oversight

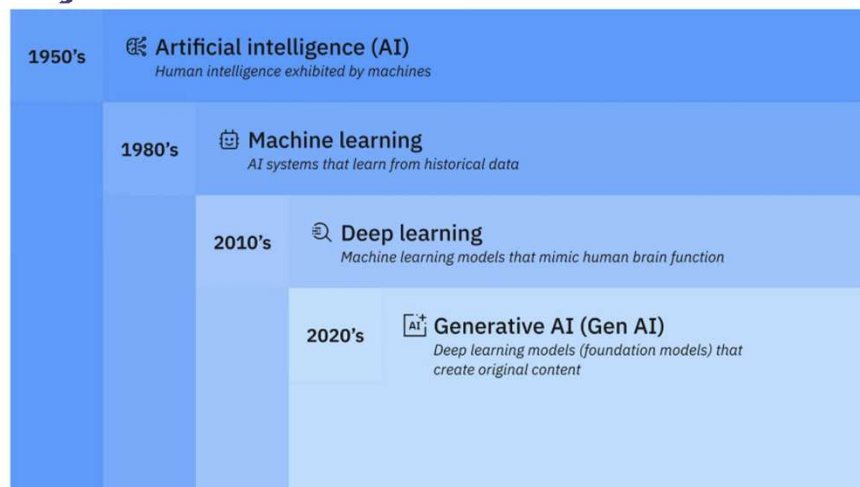


5

5

AI Generally

Brief History



Credit: What is AI? <https://www.ibm.com/think/topics/artificial-intelligence>



6

6

Why use AI?

Benefits

- Automates repetitive tasks
- Enhances decision making
- Reduces human errors
- Always available
- Minimizes physical risks



7

7

AI in Community Action

• Operations

- Scheduling
- Drafting form responses
- Fundraising
- Accounting
- Recruiting and evaluating employees

• Programs

- Facilitating intake
- Scheduling
- Tracking clients
- Collecting/analyzing data

How is your CAA using AI OR thinking about using AI?



8

8

Legal Framework

9

AI at CAAs CAPLAW Resource



AI at CAAs: Issues, Tips, & Sample AI Use Policy

Introduction

Artificial intelligence (AI) is swiftly changing our world. AI technologies are rapidly evolving systems, designed to approximate human cognition, act rationally, and perform tasks without significant human oversight.¹

Some Community Action Agencies (CAAs) have taken advantage of AI to make their services more accessible to clients, communicate with the public, and boost internal productivity. Others are more cautious about how they can ethically and responsibly step into the world of AI. Whether your CAA is looking to restrict, promote, or simply set expectations with staff with respect to AI use, an AI policy can help manage the potential risks inherent to AI use and help a CAA maintain compliance.

Disclaimer

This sample AI policy was developed by Community Action Program Legal Services, Inc. ("CAPLAW") and has not been approved by any outside authority, such as the U.S. Department of Health and Human Services. When using this sample to develop, review, or update an AI policy, CAPLAW strongly recommends you consult with legal counsel familiar with your CAA's operations and the laws of your state.

The content of this publication is intended to convey general information only and does not constitute legal advice. This publication does not constitute or create an attorney-client relationship. If you need legal advice, please contact CAPLAW or another attorney directly.

How to Use This Resource

This resource is intended to help CAAs understand the legal framework and issues that may arise in drafting and administering an AI policy. There is no one right way to address AI use at a CAA. Rather, this resource and sample policy offers a jumping off point for CAAs in the sample policy, *Revised Tip, To Do, and*

Branded text (highlight where a CAA needs to make decisions and take actions to customize the policy to its best needs the organization's needs.

¹ U.S. Government Accountability Office, *Special Committee on Artificial Intelligence, Federal Office of Cyber Policy*, *Artificial Intelligence: Overview* (February 2020).

² U.S. General Services Administration, *Guidance for Federal Agencies on Artificial Intelligence* (September 2020).

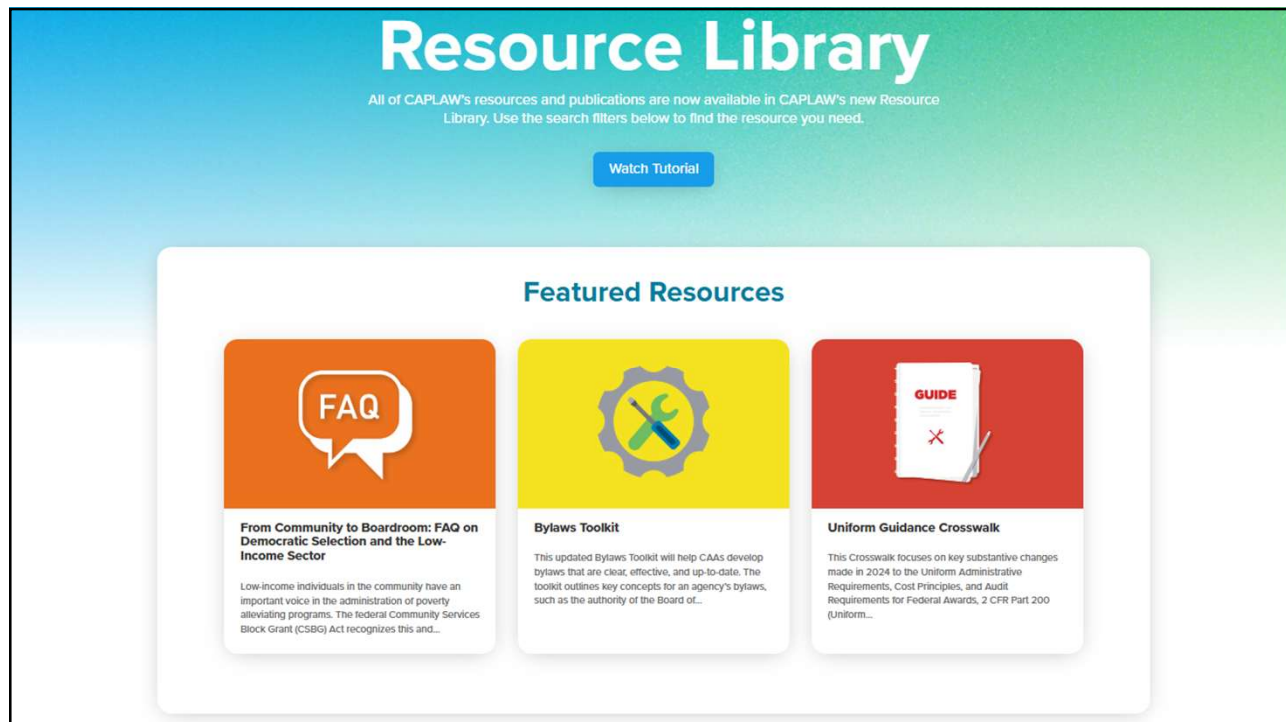


Community Action Program Legal Services, Inc.



10

10



11

Overview

- No comprehensive federal AI law
 - Some states issuing AI-specific laws
- Federal administrations issue federal agency directives
 - E.g., Executive Order (EO) 14434, *Inaugurating the Era of Super Intelligence (SI)* which replaces AI with SI
- Existing legal frameworks apply
- Legal landscape is unsettled & rapidly evolving

12

12

Overview

Potentially Applicable Laws

- | | |
|---------------------------------------|---|
| 1. Industry-specific rules | 6. Attorney client privilege & work product |
| 2. Anti-discrimination laws | |
| 3. Reasonable accommodations | 7. Intellectual property law |
| 4. Data privacy laws | 8. Labor laws |
| 5. Notice and disclosure requirements | 9. Recording laws |
| | 10. Contract law |



13

13

Legal Framework

Industry Specific Requirements

- Rules that exist for certain categories of data
 - Most comprehensive federal framework for AI use to date
 - Examples:
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Fair Credit Reporting Act (FCRA)
 - Federal Trade Commission Act (FTC)
 - Family Education and Privacy Rights Act (FERPA)



14

14

Legal Framework

Anti-Discrimination Laws

- Civil Rights Act of 1964 generally protects individuals against discrimination based on certain characteristics
 - **Title VII** prohibits adverse employment decisions based on race, color, religion, sex, and national origin
 - **Title VI** prohibits discrimination based on race, color, or national origin in programs and activities receiving federal financial assistance



15

15

Legal Framework

Anti-Discrimination Laws

- Avoid amplifying past inequities and correlating data to protected classes, if AI tool, for example:
 - Uses historical data to define employee successes
 - Assists with data inputs such as job titles, career gaps, and project assignments
 - Evaluates program eligibility
- **TIP:** (i) check quality of input and output data, (ii) be transparent about AI use, (iii) maintain human oversight



16

16

Legal Framework

Reasonable Accommodations

- Americans with Disabilities Act (ADA) requires employers to engage in an interactive process when a qualified individual with a disability requests an accommodation
 - EEOC recommends providing proactive disclosures as to how AI tools used to evaluate applicants and employees
- **TIP:** exercise caution when limiting AI tools such as AI-enabled glasses and notetakers



17

17

Legal Framework

Data Privacy

- State and federal laws govern a CAA's responsibility to protect personal information
 - E.g., funding source laws (Uniform Guidance), state data security laws (WISP in MA)
- **TIP:** review and update client consent forms (releases, etc.) to specify (i) info collected, (ii) how it will be used, and (iii) to whom it may be disclosed

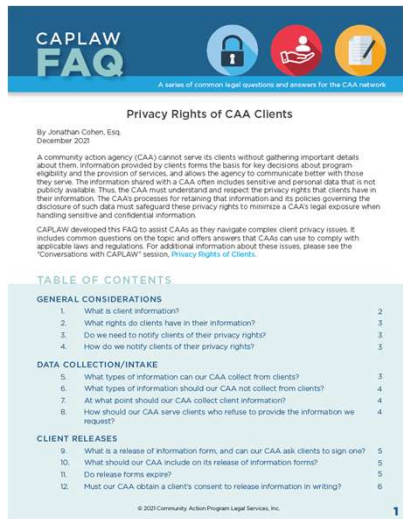


18

18

Legal Framework

CAPLAW Resource



19

Legal Framework

Notice and Disclosure Requirements

- AI mandatory disclosure laws exist in several states
 - Typically, must inform clients, employees, regulators, etc. when using AI in **decision-making** or **operations**
 - E.g., Utah's AI Policy Act requires disclosure of generative AI use when person could reasonably believe they are speaking with a human
- **TIP:** check state laws and funding source agreements before using AI chatbots or similar tools in client-facing service delivery



20

20

Legal Framework

Attorney Client Privilege + Work Product Doctrine

- State specific privilege, generally protects certain communications from discovery in a lawsuit if:
 - 1) between a client and their attorney,
 - 2) intentionally kept confidential, and
 - 3) for purpose of obtaining or giving legal advice
- Work-product doctrine provides similar protection
- If 3rd party present, protections may not apply



21

21

Legal Framework

Attorney Client Privilege + Work Product Doctrine

- AI chatbot does not qualify for attorney-client privilege
 - Missing lawyer-client relationship factor
- 3rd party disclosure of work product not an automatic waiver of protection
 - **Split in courts:** some say use of AI tool w/out direction or involvement of an attorney is not protected while others view the protection more broadly



22

22

Legal Framework

Intellectual Property Law

- Rights that exclude others from making, copying or using certain intangible creations, includes 3 forms of protection:
 - Patents
 - Copyrights
 - Trademarks
- Uniform Guidance requires certain actions if federal funds pay for intangible property
 - E.g., 2 C.F.R. § 200.315 reserves for federal agency a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or use



23

23

Legal Framework

Intellectual Property Law – Copyright

- Grants creators of original works of authorship exclusive rights in their creative work
 - Possible CAA examples: educational materials, program guides, client resources, grant reports, outreach materials
- **AI Concerns:** whether (i) assisted work is protectable and (ii) output infringes on 3rd party copyrights
 - Courts yet to recognize copyright in works lacking a human author
 - AI-assisted work may be protectable if humans determine **expressive elements** (prompts not sufficient)



24

24

Legal Framework

Intellectual Property Law – Trademarks

- Use of a word, name, or device to identify particular goods or services
 - Possible CAA examples: logos, slogans, mascots
- **AI Concerns:** whether output (i) infringes on 3rd party copyrights and (ii) is consistent with logo, brand, etc.



25

25

Legal Framework

Intellectual Property Law – Right of Publicity

- State law concept that generally creates a private right of action for unauthorized commercial use of another person's identity (i.e., name, image, likeness)
 - E.g., protects against voice and likeness misappropriations
- **AI Concerns:** use that (i) imitates voices or (ii) creates deepfakes



26

26

Legal Framework

Intellectual Property Law – Trade Secrets

- State and federal laws that generally protect info (i) the owner makes reasonable efforts to keep secret and (ii) that derives its value from not being generally known
 - Possible CAA example: donor lists
- AI output data may be protected if criteria met
- **TIP:** educate employees on what constitutes sensitive data and track capturing of potentially sensitive data by AI tools
 - E.g., AI enabled glasses inadvertently capturing internal communications



27

27

Legal Framework

Labor Law

- National Labor Relations Act (NLRA) protects employees' rights to engage in concerted activity concerning wages, hours, and working conditions
 - Possible CAA example: AI enabled glasses record audio and video of workplace conditions involving safety concerns
- **TIP:** ensure AI policy narrowly tailored and tied to legitimate business justifications



28

28

Legal Framework

Recording Laws

- States and federal consent laws to record conversations
 - Federal Electronic Communications Privacy Act and Wiretap Act requires “one-party consent”
 - Most states require “two-party consent”
- **AI Concerns:** recording (i) meetings or (ii) private conversations
 - E.g., using AI notetakers or AI-enabled glasses
- **TIP:** provide advance notice if AI tool used and use active consent prompts



29

29

Legal Framework

Contract Laws

- State law governs contracts, including with AI vendors
 - Understand data ownership, sharing, and use rights
 - Clarify data protections, security, and confidentiality
 - Review insurance, limitation of liability, and indemnification provisions
- **TIP:** before engaging vendor, vet its data practices, security measures and 3rd party disclosure policies



30

30

Legal Framework

CAPLAW Resource

CAPLAW eNews brief

Is Your Head in the Cloud? Contemplating Cloud Computing for Community Action Agencies

By Emily Center and Veronica Zhang, Esq.
August 2019

Cloud computing is rapidly increasing as one of the most cost effective and efficient ways to conduct business. A Community Action Agency (CAA) looking to add, renew, or upgrade its existing software platform is likely now more than ever to consider cloud-based solutions. As of 2012, 80% of nonprofits across the world were using some type of cloud technology, with the most frequently used services being email (55%), social networking/Internet (47%), file storage/sharing (36%), web conferencing (24%), and office productivity (23%).¹

To help CAAs better understand the benefits and risks of cloud computing, this article highlights the key differences between cloud-based applications and traditional hosted software, with a focus on the potential impact that cloud software may have on a CAA's operations and data security. It discusses reasons your CAA may decide to adopt a cloud model. Finally, the article provides a checklist of issues for your CAA to consider negotiating in its agreement with a cloud provider to ensure your CAA and its data are sufficiently protected.

What is Cloud Computing and How is it Different from Traditional Software?

Cloud computing is any application or service offered over the Internet. Examples of cloud services range from Gmail to Dropbox, Facebook, and Skype. These services are hosted at data centers all over the world, which are collectively called "the cloud." The cloud is a model for enabling convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly deployed and used with minimal management.

With traditional software, the CAA buys a specific number of licenses for each product, such as Microsoft Office, and each license typically entitles the user to physically install the software on a single computer (for example, an employee's work computer). The employee is not able to access Microsoft Office from his or her home computer or laptop, because the software is only accessible via the work computer's physical hardware.

With cloud computing, one employee with one login can access cloud-based software from anywhere with an Internet connection. The cloud allows for this flexibility because the software is kept on a remote server and managed by the cloud provider off premises, and it is simply accessed by CAA employees via the Internet.

© 2019 Community Action Program Legal Services, Inc.



Sample Policy

Sample Policy

Read and Discuss Legal Considerations



AI at CAAs: Issues, Tips, & Sample AI Use Policy

Introduction

Artificial intelligence (AI) is swiftly changing our world! As technologies are rapidly evolving systems designed to approximate human cognition, act rationally, and perform tasks without significant human oversight.

Some Community Action Agencies (CAAs) have taken advantage of AI to make their services more accessible to clients, communicate with the public, and boost internal productivity. Others are more cautious about how they can safely and responsibly step into the world of AI. Whether your CAA is looking to restrict, provide, or simply set expectations with staff with respect to AI use, an AI policy can help manage the potential risks inherent in AI use and help a CAA maintain compliance.

Disclaimer

This sample AI policy was developed by Community Action Program Legal Services, Inc. (CAPLAW) and has not been approved by any outside authority, such as the U.S. Department of Health and Human Services. When using this sample to develop, review, or update an AI policy, CAPLAW strongly recommends you consult with legal counsel familiar with your CAA's operations and the laws of your state. The contents of this publication are intended to convey general information only and do not constitute legal advice. This publication does not constitute or create an attorney-client relationship. If you need legal advice, please contact CAPLAW or another attorney directly.

How to Use This Resource

This resource is intended to help CAAs understand the legal framework and issues that may arise in drafting and implementing an AI policy. There is no one right way to address AI use at a CAA. Rather, this resource and sample policy offers a jumping off point for CAAs in the same policy. Tailoring Title, IV, Doi, and [bracketed text] highlight where a CAA needs to make decisions and take actions to customize the policy to fit their needs the organization's needs.

This resource includes a brief background of the legal framework governing AI, which is important to keep in mind when drafting an AI policy and training staff. Regular training on proper AI use and applicable legal requirements will help make any AI policy truly effective.

1. U.S. Government Accountability Office, *Report to Congress on Artificial Intelligence: Potential Effects, Guided by* (Washington: U.S. Government Accountability Office, 2020).

2. U.S. Social Security Administration, *Guidance on Artificial Intelligence* (Washington: U.S. Social Security Administration, 2020).

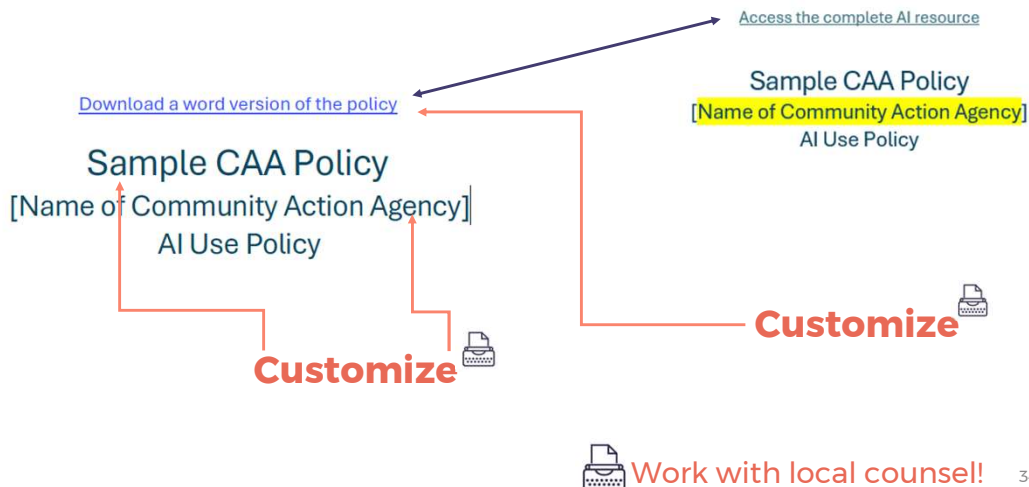


Community Action Program Legal Services, Inc.



Sample Policy

How to Use



Sample Policies

Tailoring Tips + To Dos

- [ChatGPT; Claude; Microsoft Copilot; Google Gemini; enterprise AI operating within secure environments.]

Staff wishing to use AI Tools for CAA Work should discuss the parameters of their use with [their direct supervisor or a staff member responsible for AI use oversight] (the “Supervisor”). Staff must inform the Supervisor [verbally/in writing] how the AI Tool will be used. Supervisors must approve or deny requests within [number] days.

Generally acceptable uses of AI Tools include, but are not limited to:

TAILORING TIP: Review each AI Tool and vendor’s capabilities in coordination with what the CAA’s ideal use cases are for AI use. Consider reviewing the contracts of several vendors to understand which will provide the best protections for the CAA.

TO DO: Properly train supervisors on the legal risks associated with AI use as well as the Policy’s permitted and prohibited use cases.



35

35

Sample Policy

Practical “Restricted” Approach

- Some AI use is beneficial & low-risk while still maintaining **meaningful restrictions** where they matter most:
 - Permits AI by default for low-risk activities
 - E.g., general research, brainstorming, drafting non-sensitive internal content
 - Requires supervisor approval for medium-risk activities; and
 - Prohibits AI for high-risk activities regardless of approval
 - E.g., client PII, employment decisions, legal advice



36

36

Sample Policy

Practical “Restricted” Approach

- Reasons for this approach include:
 - **Enforceability:** AI embedded in everyday tools such that a blanket prohibition is difficult monitor
 - **Shadow AI risk:** Outright prohibitions often drive AI use underground
 - **Competitive disadvantage:** As AI features become standard, restrictive policies may prevent use of tools that are increasingly necessary for efficient operations



37

37

Sample Policy

Elements

- | | |
|--------------------------------|--|
| 1. Scope | 6. Violations |
| 2. Definitions | 7. Additional Terms |
| 3. AI Use | 8. Effective Date and Revision History |
| 4. Training | 9. Exhibits |
| 5. Confidentiality and Privacy | |



38

38

Sample Policy

Scope

- Individuals covered
 - E.g., employees, board members, volunteers, contractors
- Work covered
 - E.g., all AI use by staff in connection with operations, programs, services, communications, etc.
- Potential penalties for noncompliance
 - E.g., violation may result in disciplinary action up to termination



39

39

Sample Policy

Definitions

- Terms may include: AI, AI Tool, PII, Confidential Information
- **TIP:** state and federal laws may inform definitions and language used
 - E.g., state-specific AI laws, HIPAA, Uniform Guidance



40

40

Sample Policy

AI Use

- Set baseline
 - E.g., involve a human when making decisions that affect clients, programs and communities; AI is not a decision-maker
- Establish contacts for concerns & approvals
 - E.g., consult with supervisor
 - Develop criteria/decision framework for supervisors to avoid inconsistent applications and promote uniform approvals
- Address AI tools
 - E.g., approved, acceptable, and prohibited uses; parameters of use, accuracy checks; permission process



41

41

Sample Policy

Training

- Require **all staff** to receive training before using AI tools for work
- Require **all supervisors** to receive training before approving any AI use
- Connect to existing trainings on internal IT policies
- Treat failure to receive training as a policy violation



42

42

Sample Policy

Confidentiality and Privacy

- Establish framework for assessing data inputs and protecting confidential info/PII
 - Consider classifying internal data
 - Delineate process for reviewing, approving, and inputting data depending on classification
 - E.g., tool-dependent approach that distinguishes consumer grade and enterprise tools (public Claude vs. Microsoft Copilot)
 - Develop disclosure guidelines for AI-assisted outputs (internal/external)



43

43

Sample Policy

Confidentiality and Privacy

- Data classifications may include:
 - **High risk:** PII of staff, clients, donors; immigration or legal status; health information; IP/trade secrets
 - **Medium risk:** aggregated program statistics; internal meeting notes; grant applications
 - **Low risk:** publicly available info; marketing and communications templates; training client w/out client references



44

44

Sample Policy

Other Provisions – Other Policies + Effective Date

- Effects on other policies
 - Review related policies; cross-reference and/or incorporate AI specific guidance
- Effective date
 - Consider requiring “Acknowledgments of Receipt”
- **TIP:** AI use policies are most effective when expressly integrated with CAA’s existing governance framework



45

45

Sample Policy

Other Provisions – Revision History

Effective Date and Revision History

Policy Effective Date:

Version:

<u>Revision History</u>		
<u>Version</u>	<u>Date</u>	<u>Description of Changes</u>
1.0	[]	Initial Version

TAILORING TIP: Tracking version history is a best practice for policies that may be updated more frequently, such as where technology and legal requirements are continuing to evolve.



46

46

Sample Policy

Exhibits

- May help facilitate compliance with policy
 - May provide examples of “Use Cases of AI”:
 - **Permitted uses:** general knowledge questions to understand a topic; brainstorm project ideas; create excel formulas for excel spread sheets; draft social media posts; develop/debug code
 - **Prohibited uses:** notetaking in meetings; output without human review or AI disclosure; inputting PII of staff, clients; known or should have known uses that infringe on or likely to infringe on IP or other rights



47

47

QUESTIONS?



CAPLAW | www.caplaw.org | (617) 357-6915

48

