Building Your AI Policy

Workshop Guide from Flourish and Thrive Labs

Contact: Nebu Kolenchery (nebu@fandtlabs.com)

INTRODUCTION

This worksheet will guide you through creating an AI policy framework for your organization. Work with your table to answer the questions. There are no wrong answers—this is about what makes sense for YOUR organization's needs, capacity, and risk tolerance.

PART 1: SCOPE & COVERAGE

Purpose: Define who your policy covers.

Questions to consider:

1. Who in your agency will be using AI tools?

- All staff, Specific departments, Specific roles

2. Will the policy apply to:

- All employees, Full-time employees only, Contractors, Interns

3. Are there contractors or external collaborators who need to be covered?

Your policy language: Write a Scope section of the policy – "This policy applies to…"

PART 2: DEFINING AI FOR YOUR DEPARTMENT

Purpose: Establish what "AI" means in your policy context.

Questions to consider:

1. Does your agency currently use any AI Tools?

- ChatGPT, Claude, Microsoft Copilot, Adobe AI, etc.

2. What AI tools are your staff familiar with?

3. Which types of AI should your policy address?

Your policy language: Write a Definitions section of the policy that defines concepts like AI, Gen AI, and AI tool.

PART 3: TRAINING & AWARENESS

Purpose: Ensure staff can use AI safely and effectively.

Questions to consider:

1. What AI training do you want your staff to participate in?

- Basic AI literacy (what is AI, how it works), training on approved tools, privacy and security best practices, bias and ethical training

2. How often should staff be retrained?

- Annually, when policy updates occur, when new tools are approved

3. Should there be role-specific training?

Your policy language: Write a Training section of the policy – "Before using GAI, AAI, or any AI Tool, staff must satisfactorily complete…"

PART 4: AI TOOL APPROVAL PROCESS

Purpose: Create a vetting process to ensure tools are safe and appropriate.

Questions to consider:

1. Who should be responsible for approving AI tools?

- IT Department, Privacy/Security Officer, AI Governance Committee, Department Director, Executive Leadership

2. What criteria are most important for tool evaluation?

- Data privacy and security, HIPAA compliance, accuracy, bias and fairness safeguards, compliance with records retention policies

3. How will you track and communicate which AI Tools are approved for use?

- Intranet/internal website, email announcements, policy document appendix, IT helpdesk/ticketing system

4. Do you want to define specific uses for each AI Tool?

- Example: "ChatGPT may be used for drafting internal communications but NOT for analyzing case data."

Your policy language: Write a Compliance section of the policy – "Only approved AI tools may be used by staff. AI tools will be reviewed and approved by…"

PART 5: ACCESS & REQUEST PROCESS

Purpose: Control who can access which tools and how.

Questions to consider:

1. Do you want to require staff to request the ability to use AI Tools from the approved list?

2. If yes, what is the process for staff to request access?

- Submit ticket to IT, request through supervisor, complete online form, completion of training

Your policy language: Add to the Compliance section – "Staff may request access to approved AI tools by…"

PART 6: PERMITTED & PROHIBITED USES

Purpose: Establish clear boundaries for AI use.

Questions to consider:

1. Are there specific areas where AI use should be restricted or prohibited?

- **Consider prohibiting AI for:** Clinical decisions, disciplinary actions, hiring decisions, legal determinations, processing PHI/PII
- **Consider permitting AI for:** Drafting internal communications, summarizing public health research, creating training materials, administrative tasks

Your Policy Language: Add to the Compliance section – "Approved Uses of AI Tools. AI Tools should never be relied upon for important inquiries. All outputs of AI Tools will be carefully reviewed by staff before being used in any work product. The output will not be used if it cannot be verified for accuracy. AI tools may be used for…

PART 7: DATA PRIVACY & SECURITY

Purpose: Protect sensitive information and ensure compliance.

Questions to consider:

1. Will you allow PHI or PII to be entered into any AI Tool?

2. If yes, how will you ensure compliance with HIPAA Privacy and Security Rule?

3. What data categories are absolutely prohibited?

Your Policy Language: Add to the Compliance section – "Staff must never enter the following data into AI tools…"

PART 8: ETHICAL CONSIDERATIONS

Purpose: Address bias, fairness, and responsible AI use.

Questions to consider:

1. Who is responsible for the ethical use of AI?

- We recommend this be on each of the individual staff members and requiring staff to evaluate fairness, accuracy, and cultural humility in the AI's output.

2. How do you want to address potential biases in AI tools?

- Require human review of all AI outputs, training on recognizing bias, evaluate tools for bias before approval

3. What ethical guidelines should your staff follow when using AI Tools?

- Always disclose when AI was used, verify AI outputs for accuracy

Your policy language: Add an Ethical Use Statement to the Compliance section – "When using AI tools, staff must…"

PART 9: MONITORING & ACCOUNTABILITY

Purpose: Track usage and address concerns.

Questions to consider:

1. How will the agency monitor AI tool usage?

- Usage logs/analytics, periodic audits, self-reporting, no monitoring

2. What process should be in place for reporting AI-related concerns or incidents?

- Report to supervisor, IT helpdesk ticket, privacy officer, anonymous reporting

Your policy language: Add a Reporting of Non-Compliance section – "Staff should report AI concerns or incidents to…"

PART 10: POLICY REVIEW

Purpose: Ensure the policy stays current and effective.

Questions to consider:

1. How does this AI policy interact with existing agency policies?

- Data privacy policy, Information security policy, Acceptable use policy, Records retention policy

2. How often should the AI policy be reviewed?

3. Who should review it and keep the policy up-to-date?

Your policy language: Add a Policy Review and Update section "This policy will be reviewed <frequency> by..."

PART 11: VIOLATIONS & ENFORCEMENT

Purpose: Establish consequences for policy violations.

Questions to consider:

1. What happens if a staff member violates this policy?

  • Consider difference consequences for first violation vs. serious or repeated violations

Your policy language: Add a Violations section "Violations of this policy may result in…"

PART 12: GOVERNANCE FRAMEWORK

Purpose: Coordinate AI policy across your broader government entity (county, state, etc).

Questions to consider:

1. How will your AI policy align with existing government-wide AI policies?

  • Review parent agency AI policies, ensure consistency with government IT security requirements, identify gaps or conflicts that need resolution

2. Who has the oversight authority and vision for AI in your government agency? Can you build a relationship with them and identify areas for collaboration?

3. What approvals or coordination are required from your parent government entity?

Your policy language: Add "This AI policy operates within the framework of the [parent government entity] AI governance structure. The [designated role] will serve as liaison with [government AI oversight body/person] to ensure policy alignment, coordinate on tool approvals, and maintain ongoing collaboration on AI initiatives."

Contact Information

Thank you for your use of this tool. If you would like assistance in implementing an AI policy, implementing an AI training plan, or are curious about PH360 please contact Nebu Kolenchery at Nebu@FandTLabs.com or visit us at FandTLabs.com