

## ARTIFICIAL INTELLIGENCE (AI) USE POLICY

### 1. Purpose

To guide the ethical, secure, and mission-aligned use of Artificial Intelligence (AI) technologies at OCF, ensuring compliance with data protection standards and fostering trust with donors, partners, and the community.

### 2. Scope

This policy applies to all OCF staff, contractors, volunteers, partners, and vendors who use or develop AI tools, including generative AI, predictive analytics, and automation systems.

### 3. Overarching Principles

- Accountability: Staff are responsible for decisions made using AI tools.
- Equity & Access: AI must not create barriers or inequities.
- Fairness: Avoid bias and discrimination in AI outputs.
- Transparency: Disclose AI use when appropriate.
- Reliability: Use tools that produce accurate and consistent results.
- Human Oversight: AI complements—not replaces—human judgment.
- Mission Alignment: AI must support OCF's philanthropic goals.

### 4. Data Classification & Protection

OCF classifies data into three tiers to guide responsible AI usage and ensure appropriate safeguards:

#### Tier 1 – Public or Low Risk Data

*Examples:* Public-facing program descriptions, anonymized grant summaries, published reports.

*AI Use:* Permitted with approved tools. No special approval required.

#### Tier 2 – Sensitive or Restricted Data

*Examples:* Donor names, contact details, internal financials, staff records, non-public grant applications.

*AI Use:* Requires approval from the Data Governance Committee.

*Safeguards:* Data must be anonymized or masked. External AI tools may not be used unless under a vetted agreement by the Director of Operations.

#### Tier 3 – Regulated Data

*Examples:* PII protected under law, health data (HIPAA), financial data (IRS/SEC), contractually protected donor data.

*AI Use:* Prohibited unless approved by legal counsel and the Data Governance Committee, and only with compliant tools.

*Protection Measures:* Use strong security like encryption, keep detailed records of AI activity, limit who can access the data, and make sure AI systems don't learn from sensitive information.

### 5. Training & Awareness

All OCF staff, contractors, and partners using AI tools must complete mandatory training that covers:

- Responsible AI use and ethical considerations.
- Data classification and handling protocols.
- Security practices and risk mitigation.
- How to identify and report misuse or anomalies.
- Updates on approved tools and workflows.

Training will be refreshed annually or as needed when tools or policies change.



**6. Enforcement & Non-Compliance**

Violations of this policy may result in:

- Revocation of access to AI tools or sensitive data.
- Formal review by the Data Governance Committee.
- Disciplinary action, up to and including termination of employment or contract.
- Reporting to legal authorities if the violation involves regulated data or breaches legal obligations.

OCF will maintain audit trails and conduct periodic reviews to ensure compliance and accountability.

### **Appendix A: Definitions**

**Artificial Intelligence (AI):** Technologies that simulate human intelligence, including machine learning, natural language processing, and automation tools.

**Generative AI:** AI systems that produce content such as text, images, or code based on input prompts (e.g., ChatGPT, Copilot).

**Predictive Analytics:** AI tools that analyze data to forecast future outcomes or trends.

**Automation Systems:** AI-driven tools that perform repetitive tasks without human intervention.

**PII (Personally Identifiable Information):** Data that can identify an individual, such as name, address, Social Security number, or financial account details.

**HIPAA (Health Insurance Portability and Accountability Act):** A U.S. federal law that sets standards for protecting sensitive patient health information. Under HIPAA, organizations must ensure the confidentiality, integrity, and availability of protected health information (PHI), especially when using digital tools, including AI systems.

**Compliant Tools:** AI platforms that meet legal, regulatory, and contractual obligations for data protection and security.

**Data Governance Committee:** A designated group responsible for overseeing data usage, AI approvals, and compliance at OCF.