Staff Training Manual: AI & Data Privacy for nonprofits, incorporating best practices, California compliance, and actionable steps for staff and volunteers. This manual is based on recent nonprofit sector guidance and expert recommendations.

Staff Training Manual: AI & Data Privacy

For Nonprofit Organizations (2025 Edition)

---

1. Introduction

Welcome to [Nonprofit Name]'s training on Artificial Intelligence (AI) and Data Privacy. As we adopt new technologies to advance our mission, it's critical that all staff and volunteers understand how to use AI responsibly and protect sensitive information.

---

2. Why AI & Data Privacy Matter

- **Legal Compliance:** California and federal laws (CCPA, CPRA, HIPAA) require strict protection of personal data and responsible AI use.
- **Trust:** Donors, beneficiaries, and the public trust us to handle their data ethically and securely.
- **Risk:** Data breaches or misuse of AI can result in financial penalties, reputational harm, and loss of community trust.

---

3. AI Basics for Nonprofit Staff

- **What is AI?**
  AI refers to computer systems that perform tasks typically requiring human intelligence, such as analyzing data, automating communications, or generating content.
- **How We Use AI:**
  Examples include donor analytics, automated emails, chatbots, and grant writing support.

---

4. Data Privacy Fundamentals

- **Personal Data:**
  Any information that can identify a person (name, email, health info, financial data).
- **Sensitive Data:**
  Includes health, financial, demographic, or legal status information.
- **Data Minimization:**
  Only collect and keep data that is necessary for our mission.

---

5. Safe AI & Data Privacy Practices

A. Data Collection & Use

- Collect only what you need and have consent for.
- Be transparent with stakeholders about what data you collect and why.
- Anonymize or aggregate data whenever possible.

B. Data Security

- Use strong passwords and multi-factor authentication.
- Store data securely, using encryption and access controls.

- Share sensitive data only with authorized staff.

C. Responsible AI Use

- Use only approved AI tools and platforms.
- Ensure AI outputs are reviewed by a human before acting on them.
- Regularly check for and report any signs of bias or errors in AI outputs.

D. Transparency & Accountability

- Disclose when AI is used in communications or decisions.
- Keep records of how and why AI tools are used.
- Report incidents or suspected breaches immediately to your supervisor or the data protection officer.

---

6. Compliance & Legal Requirements

- Follow all privacy laws (CCPA, CPRA, HIPAA) and organizational policies.
- Participate in regular data privacy and AI training sessions.
- Undergo annual reviews and audits of AI and data practices.

---

7. Reporting & Incident Response

- If you suspect a data breach or misuse of AI, report it immediately to [Designated Officer/IT Lead].
- Cooperate with investigations and follow the incident response plan.

---

8. Ongoing Training & Resources

- Attend all required training sessions and workshops.

- Use real-life scenarios and quizzes to reinforce learning.
- Stay updated on new policies and best practices—policies are reviewed and updated at least annually.

---

9. Questions & Support

If you have questions about AI, data privacy, or this manual, contact [Data Protection Officer/IT Lead] at [contact info].

Remember:
Your actions protect our community's trust and our organization's future. Thank you for your commitment to ethical, secure, and effective use of AI and data!

Adapted from BDO, TechSoup, NTEN, Skills4Good, and sector best practices. For more resources, see your organization's AI & Data Privacy Policy and the latest staff training materials.