RESILIENCE TECHNOLOGIES

"AI USE CHECKLIST"

for Civil Society Organisations

PRACTICAL GUIDE:

to assessing, adopting, and governing AI tools responsibly

Part 1:

Organisational Policy Considerations

Before staff can use this checklist meaningfully, your organisation needs a position on AI.

1.1 Define Your Organisation's Stance on AI

Every organisation should have a written position on AI use, even if that position is cautious or restrictive. Consider:

- *Does your organisation currently permit the use of AI tools?*
- *Under what conditions?*
- *Who is authorised to approve the use of new AI tools?*
- *Are there categories of work where AI is never appropriate (e.g. case management, legal advice, communications involving survivors)?*
- *How does AI use align with your organisational values and duty of care?*

1.2 Data Protection and Legal Obligations

- *What data protection laws apply to your organisation (e.g. GDPR, NDPR)?*
- *Does your use of an AI tool constitute data processing under applicable law? If so, is a Data Processing Agreement (DPA) required?*
- *Have you conducted or do you need to conduct a Data Protection Impact Assessment (DPIA)?*
- *Are there donor or funder restrictions on how data is handled or shared?*

1.3 Staff Responsibilities and Training

- *Do staff know what is and is not permitted when using AI tools?*
- *Is there a designated person responsible for AI governance in your organisation?*
- *Are staff trained to evaluate AI outputs critically?*
- *Is there a clear process for raising concerns about AI use?*

1.4 Accountability and Review

- *How often will your AI policy be reviewed?*
- *Who is responsible for keeping it up to date?*
- *How will incidents (data exposure, harmful outputs, misuse) be documented and escalated?*

Part 2:

AI Tool Assessment Checklist

Complete this checklist each time your organisation considers adopting a new AI tool.

Section 1

Clarify Purpose, Necessity and Organisational Policy

- ☐ *What does your organisation's policy say about the use of AI tools?*
- ☐ *Is AI the right solution for this problem, or can it be handled through safer, simpler means?*

Section 2

Identify Sensitive Data Exposure

- ☐ *Will the tool process personal, organisational, or confidential information?*
- ☐ *Does this include data related to beneficiaries, activists, or vulnerable groups?*

Section 3

Understand Data Governance and Storage

- ☐ *What does your organisation's data management plan say about data processing and storage, and does this tool align with it?*
- ☐ *Where is the data stored, and what are the platform's retention and usage policies?*
- ☐ *Is your data used to train models or shared with third parties?*

Section 4

Assess Security Risks Across Your Network

- ☐ *If one account or device is compromised, what information becomes accessible?*
- ☐ *Could the tool expose contacts, communications, or organisational relationships?*

Section 5

Evaluate the Tool's Trustworthiness

- ☐ *Who developed the tool, and what is their track record?*
- ☐ *Are there documented risks, vulnerabilities, or misuse cases?*

Section 6

Maintain Human Oversight

- ☐ *Who reviews and validates AI-generated outputs before use?*
- ☐ *Are there safeguards to prevent over-reliance on automated decisions?*

Section 7

Define Acceptable Use Within Your Organisation

- ☐ *What types of data or tasks are off-limits for AI tools? Notes:*
- ☐ *Do staff understand when not to use AI? Notes:*

Section 8

Have a Response Plan

- ☐ *What happens if the tool produces incorrect, biased, or harmful outputs?*
- ☐ *What steps will you take if sensitive data is exposed or misused?*

Part 3:

Quick Reference Red Flags

If any of the following apply, pause and seek further guidance before proceeding.

- ☐ *The tool has no clear privacy policy or terms of service*
- ☐ *The provider states that user data is used to train their models*
- ☐ *The tool stores data in a jurisdiction with weak data protection laws*
- ☐ *There is no option to request data deletion*
- ☐ *The tool has known vulnerabilities or a history of data breaches*
- ☐ *Your organization has no policy covering this type of tool*
- ☐ *Staff are already using the tool without any review process*

Glossary

AI Tool:

Any software that uses artificial intelligence or machine learning to perform tasks, including chatbots, transcription tools, translation tools, image generators, and writing assistants.

Data Processing Agreement (DPA):

A contract required under many data protection laws when a third party processes personal data on your behalf.

Data Protection Impact Assessment (DPIA):

A process to identify and minimise data protection risks before starting a new project or adopting a new tool.

Human Oversight:

The practice of having a person review, validate, and take responsibility for AI-generated outputs before they are acted upon.

Sensitive Data:

Information that could harm individuals if disclosed, including personal details, health information, location data, political opinions, and details about vulnerable groups.

This template was developed by Resilience Technologies to support civil society organisations in making safe, informed decisions about AI adoption. It should be reviewed periodically and updated in line with changes in technology, law, and organisational practice.