



Global Give Back Circle

Artificial Intelligence (AI) Use Policy

Applies To: All GGBC employees, consultants, volunteers, interns, contractors, and other individuals authorized to use GGBC systems or information

Effective Date: September 1, 2026

Review Date: March 1, 2027

Policy Status: Organizational Policy

1. Purpose

Global Give Back Circle (GGBC) recognizes that artificial intelligence (AI) tools can support innovation, efficiency, creativity, learning, program delivery, research, communications, and organizational effectiveness.

GGBC encourages responsible experimentation and appropriate use of AI while recognizing that AI tools can create risks relating to privacy, confidentiality, safeguarding, accuracy, bias, intellectual property, cybersecurity, and organizational reputation.

This policy establishes clear expectations for the responsible use of AI while ensuring that human judgment, accountability, and GGBC's values remain at the center of all work.

2. Scope

This policy applies to all GGBC employees, consultants, volunteers, interns, contractors, partners, and other individuals using AI in connection with GGBC work.

It applies whether AI is accessed through:

- Organizational devices or accounts;
- Personal devices or accounts used for GGBC work;
- Publicly available AI tools;
- Paid or organizationally licensed AI platforms; or
- AI features incorporated into other software or systems.

3. Our Approach to AI

GGBC's approach is based on six principles:

3.1 Encourage Experimentation

AI use and experimentation are encouraged.

Staff are encouraged to explore responsible ways AI can improve productivity, creativity, learning, research, program design, communications, data analysis, and organizational effectiveness.

Experimentation should take place within the boundaries of this policy and all other GGBC policies.

AI is a tool to support our work—not a replacement for professional judgment, human relationships, expertise, or accountability.

3.2 Protect Privacy and Confidentiality

Never enter sensitive or personally identifiable information into an AI tool unless the tool has been specifically approved by GGBC for that purpose.

Staff must not enter into publicly available or unapproved AI tools:

- Names or identifying information of program participants;
- Addresses, telephone numbers, email addresses, identification numbers, or other PII;
- Information about minors or vulnerable individuals;
- Safeguarding or incident information;
- Health or medical information;
- Financial or banking information;
- Passwords, authentication information, or security credentials;
- Confidential employee information;
- Confidential donor or partner information;
- Non-public contractual information;
- Confidential organizational strategy or financial information;
- Any information that could reasonably identify or expose a participant, employee, partner, or other individual.

Particular care must be taken because many GGBC program participants are adolescent girls and young women who may be particularly vulnerable to privacy, safeguarding, and reputational risks.



When AI assistance is appropriate, staff should use **de-identified, anonymized, or fictionalized information** wherever possible.

For example, instead of entering a participant's name and personal circumstances, use:

"Participant A, a 19-year-old woman from rural Kenya..."

provided that the information cannot reasonably be used to identify the individual.

When in doubt, **do not enter the information**. Consult your supervisor or the appropriate data protection lead.

4. Own Your Work

You are responsible for the quality, accuracy, appropriateness, and consequences of any work produced with AI assistance.

AI-generated content must not automatically be assumed to be accurate.

Staff remain responsible for:

- Reviewing AI-generated content;
- Fact-checking important information;
- Correcting errors;
- Checking calculations and data;
- Confirming sources and citations;
- Ensuring content reflects GGBC's values and objectives;
- Protecting confidential information;
- Identifying potential bias or inappropriate assumptions; and
- Ensuring the final work meets professional and organizational standards.

AI tools can produce incorrect, outdated, biased, incomplete, or fabricated information. Staff must exercise appropriate professional judgment before relying on AI-generated material.

The use of AI does not transfer responsibility from the employee to the technology.

5. Apply Existing GGBC Policies

AI use does not create an exception to any existing GGBC policy.

All existing policies and procedures continue to apply, including policies relating to:

- Data Protection and Privacy;
- Safeguarding;
- Cybersecurity;
- Confidentiality;
- Acceptable Use of Technology;
- Intellectual Property;
- Communications;
- Financial controls;
- Research and data integrity;
- Records management; and
- Professional conduct.

Where another GGBC policy provides a higher level of protection or a more specific requirement, the more protective or specific requirement applies.

AI must never be used to circumvent an existing policy, control, approval process, or contractual requirement.

6. Human Review Is Required

AI-generated work must receive appropriate human review before it is used for organizational purposes.

The level of review should correspond to the potential risk.

Low-Risk Uses

Examples include:

- Brainstorming;
- Developing ideas;
- Drafting internal outlines;
- Improving grammar;
- Generating non-sensitive administrative content;
- Creating generic meeting agendas.

Routine review is still required.

Higher-Risk Uses

Additional human review is required when AI is used for:

- Participant-related decisions;
- Safeguarding matters;

- Employment or HR decisions;
- Financial decisions;
- Legal or contractual matters;
- Donor communications;
- Public statements;
- Research findings;
- Program or participant data analysis;
- Grant applications or reports;
- Policies;
- External communications that could affect GGBC's reputation.

AI should **not make autonomous decisions** concerning the safety, eligibility, employment, benefits, or wellbeing of an individual.

7. Appropriate Uses of AI

Subject to this policy, appropriate uses may include:

- Brainstorming and ideation;
- Drafting and editing documents;
- Improving grammar and clarity;
- Developing presentations;
- Creating training materials;
- Developing meeting agendas;
- Summarizing non-confidential information;
- Translating non-confidential materials;
- Developing research questions;
- Creating templates and tools;
- Supporting program design;
- Developing communications concepts;
- Supporting learning and knowledge management;
- Exploring new approaches to organizational efficiency.

Staff are encouraged to identify responsible applications that can improve GGBC's effectiveness.

10. Prohibited Uses

AI must not be used to:

1. Enter or disclose confidential or personally identifiable information into an unapproved AI system.
2. Make autonomous decisions about participants, employees, safeguarding cases, or other individuals.
3. Generate or alter safeguarding records in a way that changes the factual record.

4. Create false records, evidence, quotations, data, references, or participant stories.
5. Misrepresent AI-generated material as verified research or evidence.
6. Circumvent organizational approval, procurement, security, or data protection requirements.
7. Upload passwords, security credentials, private keys, or other authentication information.
8. Use AI to impersonate another person or create deceptive communications.
9. Use AI to produce discriminatory, harassing, abusive, or otherwise inappropriate content.
10. Use AI in a manner that violates applicable law, donor requirements, contractual obligations, or GGBC policies.

11. AI and Participant Information

Because GGBC works with adolescent girls and young women, participant protection must remain a central consideration.

Staff must take particular care when using AI in connection with:

- Participant stories;
- Photos;
- Case studies;
- Testimonials;
- Safeguarding incidents;
- Mentoring records;
- Scholarship information;
- Employment information;
- Financial information;
- Educational records; and
- Any other participant data.

Participant information should be anonymized before being used with an AI tool unless the tool and use have been specifically approved under GGBC's data protection requirements.

Never assume that removing a person's name makes information anonymous.

A combination of location, age, program, circumstances, dates, photographs, or other details may still identify an individual.

12. AI-Generated Images, Audio and Video

AI-generated or AI-altered images, audio, or video must be used responsibly.

Staff must not create or alter images of participants in a way that:

- Misrepresents their experience;
- Changes the factual meaning of an event;
- Creates a misleading impression;
- Violates consent requirements;
- Compromises dignity or safeguarding; or
- Could reasonably cause harm or reputational damage.

AI-generated content must not be presented as authentic participant photography, testimony, or documentation when it is not.

Where appropriate, AI-generated or materially AI-altered content should be clearly identified as such.

13. Accuracy, Bias and Human Judgment

AI systems may reflect biases present in their training data or produce recommendations that are inappropriate for particular cultural, social, geographic, or programmatic contexts.

GGBC staff must consider:

- Cultural appropriateness;
- Gender considerations;
- Local context;
- Potential discrimination;
- Accuracy;
- Missing perspectives;
- Assumptions embedded in the output; and
- Potential unintended consequences.

AI recommendations should be treated as **input for human consideration, not as authoritative decisions.**

14. Intellectual Property and Copyright

Staff must consider copyright, licensing, confidentiality, and intellectual property when using AI-generated material.

AI-generated content should not be assumed to be free from copyright restrictions.

Staff should not upload copyrighted or confidential third-party material into AI systems unless they have the appropriate rights and authorization to do so.

Where AI produces material based on external sources, staff should verify sources and provide appropriate attribution where required.

15. AI Tools and Organizational Approval

GGBC may establish a list of approved AI tools for organizational use.

Before introducing an AI tool that will process GGBC information, staff should consider:

- Data privacy protections;
- Security controls;
- Data retention practices;
- Whether information is used to train the provider's models;
- User access controls;
- Contractual terms;
- Costs;
- Integration with GGBC systems; and
- Donor or partner requirements.

Staff should not independently purchase or introduce AI systems that process sensitive GGBC information without appropriate organizational approval.

16. Training and Learning

GGBC will encourage staff to develop responsible AI literacy.

Training may include:

- Responsible AI use;
- Privacy and data protection;
- Prompting and effective AI use;
- Fact-checking;
- Bias and ethical considerations;
- Cybersecurity;
- AI-assisted productivity;
- Appropriate disclosure; and
- Emerging AI risks.

Staff are encouraged to share successful use cases and lessons learned with colleagues.

17. Reporting Concerns

Staff should promptly report suspected misuse of AI or potential privacy, safeguarding, cybersecurity, legal, or reputational concerns to their supervisor or the appropriate GGBC lead.

Examples include:

- Sensitive information being entered into an unauthorized AI tool;
- AI-generated misinformation being distributed externally;
- Suspected participant identification;
- AI-generated content being used deceptively;
- Unauthorized use of AI for employment or participant decisions; or
- A security or privacy breach involving an AI platform.

Staff who report concerns in good faith will not be penalized for raising legitimate questions about AI use.

18. Accountability

Failure to comply with this policy may result in corrective action under applicable GGBC policies and procedures.

Serious violations involving safeguarding, privacy, cybersecurity, fraud, confidentiality, or intentional misconduct may result in disciplinary action and/or other appropriate action.

19. Management and Review

The Executive Director, or designated organizational lead, is responsible for overseeing implementation of this policy.

The policy will be reviewed at least annually and updated as AI technology, applicable laws, donor requirements, organizational needs, and recognized best practices evolve.

20. Our AI Commitment

GGBC believes responsible experimentation can make our organization stronger.



We want our staff to explore new tools, work more efficiently, learn together, and find innovative ways to improve our programs and our impact. At the same time, the people we serve must remain at the center of every decision.

Use AI boldly. Protect people carefully. Verify your work. Use your judgment. Share what you learn.

Before using AI for GGBC work, ask:

- ☐ Am I entering any personal, confidential, or sensitive information?
- ☐ Could someone be identified from the information I am entering?
- ☐ Is the AI tool approved for this type of information?
- ☐ Have I considered safeguarding and privacy risks?
- ☐ Will I personally review and verify the output?
- ☐ Could the output contain bias, inaccuracies, or fabricated information?
- ☐ Does another GGBC policy apply?
- ☐ Does a donor, partner, contract, or other external requirement apply?

When in doubt: stop, protect the information, and ask.