Responsible Use & Data Practices | UNC System Office

This guide outlines expectations, guardrails, and best practices to ensure secure, ethical, and compliant use of the Amplify platform. It supports UNC System Office values and helps staff engage AI with confidence.

Data Privacy & Classification - Version 1.0

Amplify is built for responsible experimentation — not for processing highly sensitive data.

UNC classifies data into three tiers:

- **Tier 1 (Public):** Approved for public release. Examples include press releases, published research, and university marketing materials.

- **Tier 2 (Internal):** Sensitive internal use only. Includes internal communications, non-public drafts, procedural guides, and planning documents. This tier is permitted for use in Amplify.

Tier 3 (Confidential): Legally or ethically restricted data. This includes anything covered under FERPA, HIPAA, or legal confidentiality, such as:
- Social Security Numbers

- Bank account or financial data

- Medical/health records (PHI)

- FERPA-protected student information

- Passwords or system credentials

Amplify is only approved for Tier 1 and Tier 2 data. Do not use it for Tier 3 content.

When in doubt, assume higher sensitivity and avoid entering confidential information. For full guidance, refer to the UNC Data Classification Policy or consult your department's Data Steward.

Ethical Use Guidelines

UNC supports creativity and experimentation — but transparency and accountability are key.

- Always review AI output for accuracy and tone.
- Do not use AI to generate content without human oversight.
- Avoid AI to draft evaluations, performance materials, or personnel reviews without supervisor approval.
- When creating public-facing materials, disclose AI assistance when appropriate.

Example disclaimer: "This content was drafted with the assistance of generative AI and reviewed by a UNC staff member."

Platform Protections

Amplify does not train on your data. Conversations are:

- Retained privately in your tenancy (if cloud storage is selected)
- Not accessible to external model providers
- Not used to improve public AI tools

Use "Settings" to:

- Export/delete your chat history
- Switch between local vs cloud conversation storage.

Staff Best Practices

- Use folders to organize your work.
- Name chats clearly so others can understand shared content.
- Limit copy/paste of external private data.
- Report strange AI behavior or concerns to your program lead.
- Use shared templates and assistants to reduce repetitive tasks securely.

Ongoing Support

The UNC System Office will continue refining guidance based on:

- Staff feedback
- AI platform changes
- Legal and policy developments in the UNC system and state of NC

This document will evolve. Your questions and observations are vital to shaping responsible use across the organization.

If you have questions or suggestions please contact ai@northcarolina.edu