NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

State of North Carolina

Use of Publicly Available Generative Artificial Intelligence Policy

Statewide Policy

Version 1.1

April 14, 2026

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
February 2, 2026	1.0	New	Policy Published	Office of AI & Policy
April 14, 2026	1.1	Revised	- Added clarification that agencies may set more strict requirements - Updated data classifications to match new policy	Office of AI & Policy

Document Details

Agency Name	NC Department of Information Technology
Owner	Office of AI and Policy
Title	Use of Publicly Available Generative Artificial Intelligence
Publication Date	February 2, 2026
Next Review	February 2, 2027
Document Type	PDF
Document Number	1
Version	1.1

Table of Contents

Purpose

The purpose of this policy is to provide clear expectations to state employees on the legal, responsible, and ethical use of publicly available generative artificial intelligence (GenAI) tools. This policy covers state employees' use of GenAI tools that are not provided by the State. This policy is designed to support innovation, enhance operational efficiency, and encourage thoughtful adoption of GenAI technologies, while ensuring their use aligns with applicable laws, ethical standards, data privacy requirements, and public trust. By establishing guardrails and best practices, this policy aims to encourage employees to safely leverage GenAI tools to improve productivity across state government functions.

This policy sets out the minimum requirements for the use of publicly available generative AI. Agencies may adopt this policy as their own or adopt a policy with more stringent standards applicable to their agency but must retain these minimum requirements set forth herein.

Content Lead

N.C. Department of Information Technology – Office of AI and Policy

Scope

This policy applies to all state agencies, as defined in N.C.G.S.143B-1320(a)(17).

Definitions

Publicly Available Data

For the purpose of this policy, publicly available data is data that is available and intended for public access according to state and federal law, or readily available through public sources and does not contain sensitive, personally identifiable information. Publicly available data is defined as "Public" in accordance with the State's Data Classification and Handling Policy.

Publicly Available Generative AI Tool

A publicly available generative AI tool is a form of generative AI that is made publicly available to users. Publicly available GenAI tools are not procured, licensed, or managed through the state.

Sharing Data

Sharing data includes submitting it, uploading it, or otherwise entering it into a publicly available GenAI tool.

For additional common AI definitions, reference the State of North Carolina AI Glossary.

Policy Requirements

Ethical and responsible use of publicly available generative AI requires alignment with the state's laws, policies, mission, and goals. The following guidelines are human centered with a focus on uses of AI that benefit North Carolinians and the public good.

Ensuring Responsible Data Sharing with Publicly Available GenAI Tools

- When using a GenAI tool for State work, it is imperative that employees share only **publicly available** data.
    - Employees are prohibited from sharing confidential state information/data into publicly available GenAI tools.
- Employees are prohibited from sharing personal information (PI), as defined in N.C.G.S. 75-61(10), into publicly available GenAI tools. Sharing Internal, Confidential, or Restricted data, as defined by the Data Classification and Handling Policy, in publicly available generative AI tools is prohibited.
    - Reference Table 1 for data types and risk classifications.
- Entering existing state and proprietary code into a publicly available GenAI tool is prohibited without prior approval by agency CIO and security liaison.

Reporting and Escalation

- Employees must notify supervisors and their agency security liaison of any concerns relating to AI and the use of publicly available GenAI tools.
- Employees must follow existing security policy and incident reporting protocols for suspected security breaches or data protection violations.
- Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Ensuring Appropriate Use of GenAI Tools

In order to use a publicly available GenAI tool for state work purposes, employees must:

- Complete any state and agency GenAI training.
- Ensure they are not attempting to use GenAI tools that have been identified by the state as high risk.
    - Prohibited technologies can be found in the High Risk Applications Policy.
- Ensure they are using the GenAI tool in a cloud or online environment, if using the tool on a state device. Employees must not download the tool onto state devices without special approval from ESRMO.
- Register to use the tool utilizing their state employee email address, for retention purposes. Sharing a log-in with another person is not permitted.
- Regularly review the state's publicly available generative AI guidance and best practices on the AI Corner.

Publicly Available Generative AI and Public Information

Sharing information with a publicly available GenAI tool is considered a public release of the information. Sharing non-public information with a publicly available GenAI tool can therefore violate privacy and data breach laws and regulations.

Roles and Responsibilities

NCDIT's Enterprise Security and Risk Management Office (ESRMO)

The ESRMO is responsible for:

- Maintaining a list of prohibited applications

Agency AI Oversight Committee

The Agency AI oversight committee is responsible for:

- Ensuring that employees are adhering to requirements and best practices
- Creating agency-specific policies and guidelines for the use of publicly available generative AI, including communication between an employee and their supervisor when a publicly available GenAI tool is used for state work

Employees

Employees are responsible for:

- Adhering to all the requirements and best practices included in this Policy and any agency-specific policies while using publicly available generative AI tools
- Reporting any possible misuse of a publicly available generative AI tool

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

References

Table 1 – Data Classification Summary

	Data Classification			
	Public	Internal	Confidential	Restricted
Description	Available and intended for public access.	Typically used within the agency and not for public sharing. Most documents are classified as Internal within the organization, and most employees would have access.	Often limited to a small audience on a need-to-know basis.	Represents the highest level of sensitivity and presents the highest risk if disclosed. Access to this information is restricted to a limited audience.
Types	• Information on publicly accessible websites • Routine correspondence • Employee Compensation • Press releases (final) • Job postings • Published policies, standards, procedures (excluding those related to physical or technical security) • Work email addresses	• Employee work schedules and assignments • Administrative records • Internal newsletters • Drafts of documents not yet published (press releases, draft communication, draft policies) • Training materials not created for public use • Personal email addresses • Home addresses	• Business unit plans • Security features • Sensitive public security information • Draft versions of agency's annual/quarterly reports • Forecasting assumptions • Personnel records (not compensation) • Ongoing or disposed legal proceedings and investigations • Budget information • Source code and detailed architecture • Policies and guidelines related to physical or technical security	• Personal Information • PCI Data Security Standards • PHI/HIPAA • Criminal Justice Information • State and Federal Tax Information • Conflict of Interest disclosure • Disclosed financial data • Social Security Administration-provided information • Attorney-client communications • State employee human resources records • Driver's information located within NCDMV • Controlled Unclassified Information (CUI)

Statewide Data Classification and Handling Policy, February 2025

A description of the types of data can be found below. For more information on each category, including references to General Statute, reference page 4 of the Statewide Data Classification and Handling Policy.

Internal:

1. Agency policies, standards, guidelines, and procedures not yet published (except those related to physical or technical security)
2. Drafts of yet-to-be published documents
3. Employee work schedules and duty assignments
4. Internal newsletters
5. Training materials

Confidential:

1. **State Employee Personnel Records** – Information that is confidential pursuant to N.C.G.S. 126-22.
2. **Trade Secrets** – Information that is owned by a person, has independent value derived from its secrecy and which the owner takes measures to protect from disclosure.
3. **Student Records** – The Federal Educational Rights and Privacy Act (FERPA) prohibits the disclosure of personally identifiable information derived from education records without a permissible exception defined by the law.
4. **Security Features** – Information that describes security features of electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems, including hardware or software security, passwords, or security standards, procedures, processes, configurations, software, and codes.
5. **Sensitive Public Security Information** – Information containing specific details of public security plans and arrangements or the detailed plans and drawings of public buildings and infrastructure facilities.
6. **Financial and Strategic Planning Records** - Information related to agency financial projections, budgets, legal proceedings and investigations not covered by attorney-client privilege or work product and forecasting assumptions is confidential.

Restricted:

1. **State and Federal Tax Information (FTI)** – Any return or return information received from the Internal Revenue Service (IRS) or secondary source, such as from the Social Security Administration (SSA), Federal Office of Child Support Enforcement, or the Bureau of Fiscal Service.
2. **Payment Card Industry (PCI) Data Security Standard (DSS)** – Confidential credit card information including credit card magnetic stripe data, card verification values, payment account numbers, personal identification numbers, passwords, and card expiration dates.
3. **Protected Health Information (PHI)** – Confidential health care information for natural persons related to past, present, or future conditions, including mental health information.
4. **Criminal Justice Information (CJI)** – Data necessary for law enforcement and civil agencies to perform their missions including but not limited to biometric, identity history, biographic, property, and case and incident history data.
5. **Social Security Administration (SSA) Provided Information** – Information that is obtained from the SSA. This can include a Social Security number verification indicator or other PII data.
6. **Driver's Privacy Protection Act (DPPA)** - DPPA definition applies exclusively to data maintained by the North Carolina DMV and dictates permissible disclosures and uses under federal law. This law defines "personal information" and "highly restricted personal information" in a manner distinct from North Carolina's Statewide Data Classification and Handling Policy.
7. **Controlled Unclassified Information (CUI)** - Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable Federal law, regulations, and government-wide policies.
8. **Personal Information** - A person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b).