

# Data privacy and security

What information can enter which AI systems?

Make the rule specific enough for someone facing an actual document, conversation or student record.

## Recommended starting position

Apply institutional data classifications to prompts, uploads, retrieved records, outputs and logs. Permit protected information only through an explicitly approved tool and use case with appropriate legal, contractual and technical controls. Minimize information and permissions.

Removing a name may leave enough context to identify someone. A meeting transcript can mix student, employee and partner information. A connector can expose more than a user intended to upload. Privacy review and security review must cover the entire information flow.

## What the evidence supports

Carteret restricts protected information in public AI tools. Purdue ties sensitive-data use to approval. FERPA provides the official starting point for education-record obligations; applying it requires attention to the specific information and disclosure.

## Establish these foundations

- Identify the information category and permitted purpose.
- Check access, vendor reuse, retention, deletion and subcontractors.
- Publish an incident route people can use immediately.

## The choices to make locally

### Public or approved synthetic information

Consider this when: The task can be completed without real confidential records.

Tradeoff: Confirm the material is genuinely suitable for the intended use; public availability does not settle intellectual-property rights.

### Protected information in a controlled use

Consider this when: There is an approved need and the required safeguards are established.

Tradeoff: Requires review of authority, agreements, configuration, access and monitoring.

### Keep the information out

Consider this when: The purpose, authority or controls cannot be established.

Tradeoff: Offer a workable approved alternative and a review route so staff can complete the underlying task.

## **Illustrative campus case**

### **An AI note-taker joins a student-support meeting.**

A staff member invites a note-taker to help prepare an action summary. The conversation includes disability accommodations, academic progress and a partner placement.

Convenience does not resolve who may receive the information, how the recording is used or what participants were told.

1. Check the approved meeting use, information categories and recording requirements before enabling it.
2. Confirm participation choices, retention, access and any applicable consent or disclosure requirements with responsible offices.
3. If approval is unresolved, use an authorized human note-taking process and share only the necessary action summary.

What the team produces: A usable meeting rule and a documented information-handling decision.

## **Who is responsible**

Board and trustees: Ask how leadership knows that protected information is kept within approved uses.

Institutional leaders: Make data ownership and incident authority explicit, with resources to enforce them.

AI task force: Connect plain-language rules to privacy, security, records, procurement and partner requirements.

## **Illustrative language to adapt**

Users must not place protected institutional information in an AI system unless the tool and the specific use are authorized for that information. Approval must address permitted processing, access, retention, vendor reuse, subcontractors, deletion and incident response. Only the information and permissions needed for the approved purpose may be provided.

Read alongside model policy sections 5, 9, 11. Reconcile local authority and requirements before adoption.

## **Evidence of implementation**

- An information-flow description covering inputs, retrieval, output and logs.
- Documented authority and relevant contractual and security controls.
- A tested incident route and an owner who can contain exposure.

Reconsider when: Reassess when information categories, connectors, retention, vendor reuse or the people with access change.

## **Supporting sources**

[Carteret Community College / Artificial Intelligence Policy](#)

[Purdue University / Artificial Intelligence Use](#)

[US Department of Education / FERPA regulations and guidance](#)