

Tools, use cases and vendors

What exactly does an approval authorize?

An approved product still needs a defined purpose, appropriate data and clear operating boundaries.

Recommended starting position

Make approval specific enough to be usable: tool, use case, information, users, permissions and conditions. Offer a simple route for routine, low-risk uses and specialist review for consequential uses, protected information and connected actions.

A campus subscription does not answer whether a particular feature may access personnel records, evaluate students or send messages. Permission can become ambiguous when a vendor introduces new features inside an existing product.

What the evidence supports

Purdue requires both tool and use-case approval for sensitive or restricted data. RPCC maintains an approval and governance process. These are concrete precedents for treating the intended use as part of the approval decision.

Establish these foundations

- Give employees a clear way to find approved uses and conditions.
- Review the vendor relationship and the actual information flow.
- Require reassessment for a material change in access, purpose or capability.

The choices to make locally

Pre-authorized routine uses

Consider this when: The use stays within defined low-risk boundaries and permitted information.

Tradeoff: Reduces delay, but requires understandable boundaries, examples and a way to ask about exceptions.

Bounded pilots

Consider this when: The institution needs evidence before broader adoption.

Tradeoff: Set owners, limited access, success measures, review dates and a way to stop or exit.

Individual review

Consider this when: The use affects rights, sensitive information, important decisions or external actions.

Tradeoff: Needs specialist capacity and an escalation route so review does not stall indefinitely.

Illustrative campus case

A familiar platform adds an AI feature.

An employee sees a new assistant inside a college-licensed platform. It can summarize files across connected folders. The employee assumes the existing subscription approves the feature.

The question is whether the new feature changes access, processing or vendor data use.

1. Confirm which information the feature can retrieve, including inherited permissions.
2. Check contractual terms, retention, training use and controls for the new capability.
3. Publish the approved scope or keep the feature restricted while review is unresolved.

What the team produces: An approved-use entry that staff can understand and specialists can verify.

Who is responsible

Board and trustees: Request assurance that consequential deployments enter an accountable review process.

Institutional leaders: Assign approval authority, review capacity and a route for timely escalation.

AI task force: Make the review process coherent across procurement, IT, privacy, accessibility and the affected service.

Illustrative language to adapt

Approval of an AI product does not authorize every use of that product. The approving authority must specify permitted purposes, information, users and capabilities, together with review conditions. Material changes to those conditions require reassessment before expanded use.

Read alongside model policy sections 4, 5, 9, 12. Reconcile local authority and requirements before adoption.

Evidence of implementation

- An accessible list of approved uses and restrictions.
- Contract and technical review proportionate to the deployment.
- A named owner, review date and exit arrangement.

Reconsider when: Review new integrations, vendor changes, expanded data access, new populations and features that can initiate actions.

Supporting sources

[Purdue University / Artificial Intelligence Use](#)

[River Parishes Community College / Use of Artificial Intelligence](#)