

AI data journey mapping

Compare data flows through different AI systems to make informed decisions about AI tools oversight in educational settings.



Engage: See where your data goes when you use AI tools

Understanding where your data goes

Instructions:

For each scenario below, we'll tell you what actually happens to your information when you use different AI tools. Then you'll mark the potential risks:

- Add an  where you think data could be at risk.
- Add a  where the tool protects your data.

What could go wrong with your data?

Here are the main things to watch out for:

- **Device security:** Someone could access your phone, iPad, or computer.
- **Data transmission:** Your information could be intercepted while traveling to company servers.
- **Server security:** The company's servers could get hacked.
- **Data storage:** Companies might keep your data longer than they promised.
- **Employee access:** Company staff might be able to see your personal information.
- **Training purposes:** Your data might be used to make AI better for other users.

AI data journey mapping

Engage: See where your data goes when you use AI tools (continued)

Scenario A: Using Writing Tools with Apple Intelligence

Situation: You're using Apple Intelligence Writing Tools to help proofread an email to parents about a field trip.

What actually happens: Apple Intelligence first tries to process your request right on your device. If it needs more processing power, it sends your text to Apple's Private Cloud Compute servers, where it's processed and immediately deleted. Apple can't access your data, and it's never stored or used to train other AI models.

Mark each risk with a  (protected) or  (at risk):

- ☐ **Device security:** Someone could access your phone, iPad, or computer.
- ☐ **Data transmission:** Your information could be intercepted while traveling to company servers.
- ☐ **Server security:** The company's servers could get hacked.
- ☐ **Data storage:** Companies might keep your data longer than they promised.
- ☐ **Employee access:** Company staff might be able to see your personal information.
- ☐ **Training purposes:** Your data might be used to make AI better for other users.

Scenario B: Using ChatGPT for lesson planning

Situation: You paste a unit overview into ChatGPT.com and ask it to suggest engaging activities for eighth graders.

What actually happens: Your text is sent to OpenAI servers where it's processed by their AI model. By default, your conversations may be used to improve their AI systems (though you can opt out). The data is stored on their servers according to their retention policies.

Mark each risk with a  (protected) or  (at risk):

- ☐ **Device security:** Someone could access your phone, iPad, or computer.
- ☐ **Data transmission:** Your information could be intercepted while traveling to company servers.
- ☐ **Server security:** The company's servers could get hacked.
- ☐ **Data storage:** Companies might keep your data longer than they promised.
- ☐ **Employee access:** Company staff might be able to see your personal information.
- ☐ **Training purposes:** Your data might be used to make AI better for other users.

Engage: See where your data goes when you use AI tools (continued)

Scenario C: Using face detection in Photos

Situation: Your iPhone automatically creates collections and memories in the Photos app based on faces of people and pets in your photos and videos.

What actually happens: The Photos app uses on-device machine learning to organize your photos and videos in ways that are meaningful to you. This happens entirely on your device and includes recognizing scenes, identifying people and pets, analyzing photo quality, and even classifying audio. Apple doesn't access your photos or videos, and doesn't use them for research and development.

Mark each risk with a  (protected) or  (at risk):

- ☐ **Device security:** Someone could access your phone, iPad, or computer.
- ☐ **Data transmission:** Your information could be intercepted while traveling to company servers.
- ☐ **Server security:** The company's servers could get hacked.
- ☐ **Data storage:** Companies might keep your data longer than they promised.
- ☐ **Employee access:** Company staff might be able to see your personal information.
- ☐ **Training purposes:** Your data might be used to make AI better for other users.

AI data journey mapping

Investigate: What you need to think about when choosing AI tools

Compare the three AI scenarios

Now that you've looked at how each tool handles your data, fill out this comparison chart for the three scenarios you just explored.

	Scenario A: Apple Writing Tools	Scenario B: ChatGPT for lesson planning	Scenario C: Face detection in Photos
What type of AI is this? classical machine learning, generative, both			
How does it handle data? stays on my device, goes to company servers, not sure, mix of both			
What agency does it have? low (follows rules), medium (makes some choices), high (makes creative decisions)			
How transparent is it? invisible, somewhat visible, very clear when it's working			

AI data journey mapping

Investigate: What you need to think about when choosing AI tools (continued)

	Scenario A: Apple Writing Tools	Scenario B: ChatGPT for lesson planning	Scenario C: Face detection in Photos
Does it align with your values? strongly aligns, mostly aligns, neutral, some concerns, major concerns			
How much attention does it need from you?  Low: Accept defaults, use as intended, minimal monitoring  Medium: Understand what it does, review outputs in some cases, consider context  High: Always review outputs, understand privacy implications, make intentional decisions about when/how to use			

AI data journey mapping

Act: Make your data decisions

Your personal AI guidelines

Based on what you've discovered about how different AI tools handle data, create your own guidelines for choosing AI tools in your classroom.

For my classroom, I want AI tools that:

- ☐ Keep data on my device when possible
- ☐ Have clear policies about deleting data
- ☐ Don't use student information to train other AI models
- ☐ Tell me clearly where my data goes
- ☐ Let me opt out of data collection
- ☐ Other: _____

I'll avoid AI tools that:

- ☐ Have confusing or unclear privacy policies
- ☐ Store data forever without a good reason
- ☐ Use student data to improve AI for other users
- ☐ Don't let me delete or control my data
- ☐ Ask for personal information they don't need
- ☐ Other: _____

Think it through:

- How did exploring these data paths change your thinking about different AI tools?
- Which AI features are obvious when they're working? Which are hidden? What does that mean for you and your students?
- Now that you understand these differences, how might you introduce AI tools to your students?
- How would you explain these privacy concepts to students or parents?
- What questions do you still have about AI and data privacy?