Custom GPT Security & Responsible Use Checklist

Looking to build and use your own custom GPTs? Follow this checklist to make sure you're being safe and responsible with data and privacy requirements.

1. Data Privacy & FERPA Safeguards

Am I avoiding the use of student names, IDs, or personally identifiable information (PII)?
Am I summarizing data or examples instead of pasting real internal communications?
Have I confirmed that no uploaded files contain sensitive info (e.g., HR reports, complaints, grades)?
If my GPT processes sensitive content (even summaries), have I run it by legal/IT?

2. Document & File Uploads

Are the uploaded documents cleared for general staff/internal use?
Am I only using final or published versions of policies, SOPs, or handouts?
Have I removed metadata, tracked changes, or private notes before uploading?
If the GPT is being shared across teams, does everyone know what's in the documents?

3. Governance & Team Collaboration

Am I using ChatGPT Teams to manage access securely (vs. a personal account)?
Have I limited edit permissions to the right builders or reviewers?
Is there a version control process or naming convention (e.g., v1.0, v2.1)?
Do I have a point person responsible for reviewing and updating this GPT quarterly?

4. GPT Behavior & User Guidelines

Are the GPT instructions clear about what not to do? (e.g., Don't answer legal questions)
Did I include disclaimers or reminders inside the GPT instructions or conversation starters?
Is it clear who the GPT is for, and what it's not designed to do?
Have I trained my team to treat GPT output like a draft or assistant—not a final decision?

5. Communications & Rollout

Am I sharing this GPT with a clear 'how to use it' explainer?
Have I given people a safe place to provide feedback, ask questions, or raise concerns?
Have I scheduled a check-in 30–90 days after rollout to evaluate adoption, risks, and updates?
Does this tool make life easier, safer, or more consistent for my team?

Remember:

Just because it's private doesn't mean it's secure. Just because it's useful doesn't mean it's safe.

Have a conversation with your data security team or CTO to make sure you're in compliance of your institution's policies and procedures before taking on GPT projects or using new AI tools or features.