Version 1.0 Last update: March 3, 2026

University of Texas System
UT Aspire
Quick Reference

UT Aspire – Quick Reference

This section provides a concise summary of recommended practices to help users work effectively in UT Aspire while reducing the likelihood that HiddenLayer or native guardrails will take action on prompts or responses.

Recommended Practices

- Clearly state your goal, intended audience, and desired output format.
- Provide legitimate context and request high-level, defensive, or policy-based guidance when working with sensitive or security-related topics.
- Use only published or anonymized data and redact sensitive details before pasting content.
- Break complex requests into smaller steps and refine iteratively.
- When unsure, ask UT Aspire to ask clarifying questions before generating a response.

Things to Avoid

- Requests that imply bypassing controls, evasion, exploitation, or wrongdoing.
- Step-by-step instructions that could be misused outside a legitimate context.
- Entering secrets, tokens, private keys, production configuration values, or confidential or controlled data.
- Repeating a blocked prompt without reframing it for safer, higher-level output.

If a Prompt Is Blocked or Redacted

- Re-state your legitimate intent and request a high-level or defensive alternative.
- Ask for best practices, checklists, summaries, or conceptual explanations instead of operational detail.
- If you believe the action is a false positive and would like it investigated, contact your campus or institution IT/support staff and work with them to submit a ServiceNow ticket on your behalf in the UT Shared Information Services (SIS) ServiceNow instance under the Generative Artificial Intelligence (GenAI) category. Include the time, model, and a redacted copy of the prompt or response.

Revision History

Version	Description	Revision Date
1.0	Initial Version	March 3, 2026