UTEP Standard 25: Acceptable use of AI Tools

This AI Use Standard lays out best practices for using AI while protecting sensitive data, whether institutional, personal, or proprietary. As things continue to evolve, expect further updates.

Allowable Use:

When publicly available tools like ChatGPT or Google Gemini are used, any data entered can be used to train the corresponding large language model as if it were published. The university provides access to AI tools that contractually safeguard your information and ensure it remains protected from public disclosure. The University's Microsoft Campus Agreement includes the necessary data protections, to include not using customer data to train their models. As a result, you can use university data in the university instance of Microsoft Co-Pilot and protect that data from public disclosure.

The following guidance outlines the types of data that may be used with AI tools in accordance with the UTEP Information Security Standard 9 - Data Classification Standard and relevant university polices.

- **Public or Published Data:** Data that is publicly available or classified as Published university information, as defined by the UTEP Information Security Standard 9 - Data Classification Standard (DCS), may be used freely with all AI tools.
- **Controlled or Confidential Data:** Data classified as Controlled or Confidential university information, as defined by the UTEP Information Security Standard 9 - Data Classification Standard (DCS), can be used with AI tools that are managed by the university and covered by contracts explicitly protecting university data. These contracts should ensure that the data is **NOT** used to train the corporation's models. It should also ensure data is isolated in a separate instance inaccessible to external parties.
- **Acceptable Use**: In all cases, use should be consistent with the Acceptable Use Policy.

Prohibited Use:

- **Unauthorized AI Tools:** AI tools that lack a university contract and appropriate data-sharing controls are not approved for use with **Controlled** or **Confidential** university data, as defined by the UTEP Information Security Standard 9 - Data Classification Standard (DCS). This includes free or non-UT-managed versions of AI tools like ChatGPT and Copilot.
- **Sensitive Information:** Student records subject to FERPA, proprietary information, and any other data classified as **Confidential** or **Controlled** must not be used with AI tools that are not contracted with the university and protected.

- **Non-Public Output:** Unauthorized AI tools should not be used to generate non-public outputs, such as proprietary or unpublished research, legal analysis or advice, recruitment or personnel decisions, academic work when prohibited by instructors, creation of non-public instructional materials, or grading.

Additional Guidance:

- **Personal Liability:** Accepting click-through agreements without delegated signature authority may result in personal responsibility for compliance with the terms and conditions of the AI tool.
- **Vendor and Third-Party Compliance:** When engaging with AI tools provided by external vendors, ensure compliance with UTEP Information Security Standard 22, which outlines requirements for vendor and third-party controls and compliance.
- **Standardized Notice:** University is required by state rules to ensure that any AI system deployed or used, if it interacts directly with the public or is a controlling factor in a consequential decision, includes a standardized notice. More information on that notice will be forthcoming.
- For more information on the use of AI Tools for teaching and learning, please see the following guidance from the Office of the Provost.
- For more information on the use of AI tools for Research, please see the following for guidance from Research & Innovation.

Guidance on Appropriate Use

For questions regarding the appropriate use of AI Tools, please contact the UTEP Information Security Office at security@utep.edu.

AI Information Sharing Group

Co-Chairs
Luis Hernandez – Vice President for Information Resources
Dr. Salamah Salamah – Associate Vice President, Research & Innovation

Members
Dr. Amanda Vasquez-Vicario – Vice President for Enrollment Management
Dr. Beth Brunk – Dean, Extended University
Dr. Clifton Tanabe – Dean, College of Education
Dr. Victoria Suttmiller – Assistant Vice President, Student Affairs
Dr. Cauam Ferreira Cardoso – Director, Institute for Applied AI Innovation
Iris Niestas – Assistant Vice President, Budget and Payroll
Frank Poblano – Associate Vice President, Information Resources
Edgar Luna – Assistant Vice president, Information Resources