جامعة فهد بن سلطان
FAHAD BIN SULTAN UNIVERSITY

AI Acceptable Use Policy

Policy #:	IT-920	Revision #:	01
Accessibility level:	Internal	Effective date:	Oct. 2026

1. Purpose

This policy sets out the rules for the use of AI tools at FBSU so that faculty, staff, students and contractors can benefit from AI without exposing FBSU data, breaching the Personal Data Protection Law (PDPL) or other applicable laws and regulations of the Kingdom of Saudi Arabia or compromising academic integrity, in line with the AI Ethics Principles issued by the Saudi Data and Artificial Intelligence Authority (SDAIA).

2. Scope

This policy applies to everyone who handles FBSU data or uses FBSU systems: faculty, staff, students when they use FBSU systems or handle FBSU data, contractors, vendors and programmers. It covers every AI tool — chatbots, assistants built into office software, code assistants, translation, transcription, image and video tools, browser extensions and AI features in third-party systems — whether used on FBSU or personal devices, with institutional or personal accounts. The use of AI in scientific research is also governed by the Policy on the Use of Generative Artificial Intelligence in Scientific Research (SR-700); where both policies apply, the stricter requirement prevails.

3. Definitions

The following terms shall have the meanings assigned to them below wherever they appear in this policy.

3.1. **AI Tool:** Any software or service that generates, summarizes, translates, classifies or analyses content using machine learning, including features built into other products.

3.2. **Approved AI Tool:** A tool listed on the FBSU Approved AI Tools List, used through an FBSU-managed account under the settings approved by the IT Center.

3.3. **Public AI Tool:** Any AI tool not on the approved list, or any tool used through a personal account.

3.4. **Upload:** Typing, pasting, attaching, dictating, screen-sharing or connecting any content to an AI tool, including through plug-ins, connectors or API calls.

3.5. **FBSU Data:** Any data, document, record, source code, configuration, image, recording or other artifact created, received or held by FBSU, in any form.

3.6. **Personal Data:** As defined in the PDPL; includes student, applicant, employee and patient data.

3.7. **Classification Levels:** Top Secret, Secret, Confidential and Public, as defined in the National Data Governance Interim Regulations and the NDMO Data Classification Policy, and applied through the FBSU data classification process.

3.8. **Deepfake:** Image, audio or video content generated or manipulated by AI that realistically depicts a real person saying or doing something that the person did not say or do.

4. Policy

4.1. **Approved tools only:** FBSU business may use only approved AI tools, through FBSU-managed accounts. The IT Center keeps the Approved AI Tools List and adds a tool only after a security, privacy and hosting review. Approval requires, at least: no training on FBSU data; defined data retention, and deletion; administrator controls and logs; contractual confidentiality commitments; a data protection impact assessment by the IT Center where the tool processes personal data; and hosting within the Kingdom for any tool that will process personal or Confidential data. Any transfer of personal data outside the Kingdom must comply with the Regulation on Personal Data Transfer outside the Kingdom.

4.2. **Data that may be uploaded by classification level:** The following rules apply:

a. **Public** data (published catalog, public announcements, published research): allowed in public AI tools and in approved AI tools.

b. **Confidential** data (internal reports, drafts, unpublished exams, student or staff personal data, contracts): **prohibited** in public AI tools; allowed in an approved AI tool only where the tool is approved for Confidential data, and only the minimum needed.

c. **Secret** data: **prohibited** in public AI tools; **prohibited** in approved AI tools unless the **Institutional Digital Transformation Committee (IDTC)** approves in writing and the tool is hosted on FBSU-controlled infrastructure or within the Kingdom. Top Secret data: prohibited in all AI tools.

Data that has not yet been classified in accordance with the FBSU data classification process shall be handled as Confidential for the purposes of this policy until it is classified.

4.3. **Always prohibited in any AI tool not approved for that purpose:** The following must never be uploaded:

a. Student records: names with IDs, grades, transcripts, attendance, disciplinary or health information, and student work that identifies the student.

b. Applicant files, national ID or Iqama numbers, passport copies, photos.

c. HR, payroll, salary and performance data.

d. Exam questions and answer keys before the exam is held.

e. Unpublished research data, and human-subject research data, in accordance with Policy SR-700.

f. Financial records, contracts, tenders and legal correspondence.

g. Passwords, keys, tokens, connection strings, database dumps, network diagrams and system configurations.

h. Official letters and decisions before they are issued.

i. Sensitive Data as defined in the PDPL.

j. Manuscripts, proposals or reports received in confidence for peer review, in accordance with Policy SR-700.

k. Third-party content provided to FBSU under a confidentiality agreement or license that does not permit its use in AI tools (e.g., accreditation reviews, licensed databases and e-resources).

4.4. **Source code and systems:** Programmers and vendors must not paste or upload FBSU source code, database schemas, logs or configurations into public AI tools or code assistants, and must not push FBSU code to public repositories. Code assistants may be used only if approved, through FBSU accounts, with code-sharing for model training turned off. AI-generated code must be reviewed and security-tested before it enters any FBSU system.

4.5. **Connecting AI to FBSU systems:** No AI tool, plug-in, browser extension or agent may be connected to FBSU email, storage, the student information system, LMS or databases without written IT Center approval. AI meeting assistants may record or transcribe an FBSU meeting only with the approval of the meeting chair and after all participants have been informed.

4.6. **Human responsibility:** Users remain responsible for anything they produce with AI. AI output must be checked for accuracy and bias before use. AI must not be the sole basis for decisions on admissions, grades, discipline, hiring or any other decisions about individuals.

4.7. **Teaching, learning and research:** Faculty set and state the permitted AI use for each course and assessment in the course syllabus. Students must disclose any AI use in the manner specified by the instructor; undisclosed or prohibited use is treated as academic misconduct under FBSU academic integrity regulations. Researchers must comply with Policy SR-700, including the in-paper declaration of AI use and the limit on AI-generated content, in addition to any publisher requirements, and must not upload participant data to public AI tools.

4.8. **Transparency:** Content produced largely by AI and published in FBSU's name must be reviewed by an accountable person before release.

4.9. **Intellectual property:** Users must respect copyright and license terms when using AI tools, in accordance with the Copyright Law of the Kingdom and FBSU intellectual property regulations, and must not present AI-generated content as their own original work without disclosure.

5. Roles and Responsibilities

5.1. **Institutional Digital Transformation Committee:** Recommends this policy for approval by the University Council; approves exceptions; reviews AI risks quarterly.

5.2. **IT Center:** Keeps the Approved AI Tools List; configures accounts; monitors AI traffic; blocks high-risk services.

5.3. **IT Center (Data Protection):** Assesses AI tools that process personal data; handles AI-related data incidents and any required transfer assessment.

5.4. **System owners and department heads:** Ensure their teams follow this policy; confirm compliance each year.

5.5. **Deanship of Graduate Studies and Scientific Research and college deans:** Oversee the use of AI in research under Policy SR-700, and in teaching and assessment under FBSU academic regulations.

5.6. **All users:** Follow this policy; complete AI awareness training; report incidents.

6. Disclosure, Incidents and Compliance

6.1. **Disclosure of past use:** On this policy's effective date, every user must disclose any Confidential or higher-classified FBSU data, documents, code or other artifacts uploaded to AI tools in the past, through the form issued by the IT Center. The disclosure lets FBSU assess and limit exposure, for example by requesting deletion from the provider and rotating exposed credentials.

6.2. **Incidents:** Uploading Confidential or higher-classified data, or any personal data, to a public AI tool is a data incident. Report it to the IT Center-immediately; it is then handled under the Data Breach Response Plan (AA-405-F01) and the PDP Policy, including notification to SDAIA within 72 hours of becoming aware of the breach, and notification of affected data subjects, where required by the PDPL and its Implementing Regulations.

6.3. **Monitoring:** FBSU may monitor network traffic to AI services from FBSU networks and devices to enforce this policy, in line with applicable law.

6.4. **Compliance:** Breaching this policy may lead to loss of access and disciplinary action under FBSU regulations. Contractors and vendors who breach it may face contractual penalties.

6.5. **Exceptions:** Exceptions must be requested in writing to the IT Center and approved by the IDTC, for a defined period.

6.6. **Review:** The IT Center and the IDTC review this policy annually, or sooner if national AI or data regulations change.

7. Policy Ownership and Approval

7.1. **Policy owner:** Information Technology Center.

7.2. **Reviewed by:** Institutional Digital Transformation Committee (IDTC)

7.3. **Approved by:** University Council.

7.4. **Date of approval:** 18-October-2026.

8. Related Documents

8.1. Personal Data Protection Law (PDPL) and its regulations, including transfer of personal data outside the Kingdom

8.2. SDAIA General Data Sovereignty Policy, AI Ethics Principles, and Generative AI Guidelines

8.3. NDMO National Data Governance Interim Regulations and Data Management and Personal Data Protection Standards, including the Data Classification Policy

8.4. NCA Essential Cybersecurity Controls (ECC)

8.5. FBSU Personal Data Protection Policy (AD-095, sections 8.17 and 8.21–8.23)

8.6. Access Control Policy (AD-304)

8.7. Code of Conduct Policy (AD-109)

8.8. Data Breach Response Plan (AA-405-F01)

8.9. FBSU Approved AI Tools List

8.10. Copyright Law and its Implementing Regulations

8.11. Use of Generative Artificial Intelligence in Scientific Research Policy (SR-700)

8.12. FBSU Academic Integrity regulations