SMU Student AI Tools and Data Use Guidelines

AI Tool	Tool Licencing	Types of Data		
	University-licenced	Data from Websites or other Publicly Available Sources	SMU Data Classified "Unrestricted" and "Restricted"	SMU Data classified "Sensitive" to "Highly Sensitive" Data, PD
SMU Studio Chat ^	Yes	Yes	Yes	Permission Required on AI use case*. Anonymise all personally identifiable data.
Microsoft 365 Copilot Premium (Work option) ^	Yes	Yes	Yes	Permission Required on AI use case*. Anonymise all personally identifiable data.
Google Workspace for Education Plus including Google NotebookLM	Yes	Yes	Yes	Permission Required on AI use case*. Anonymise all personally identifiable data.
MS 365 Copilot Basic (Web option)^	Yes	Yes	No	No
Lumi Pro – Fully integrated and grounded on course materials (LLM Claude)	Yes	Yes	Yes	Permission Required*
Other SMU Specially licenced AI Tool ^	Yes	Yes	Yes	Permission Required on AI use case*. Anonymise all personally identifiable data.
Any Free AI or GPT Tool	No	Yes	No	No
Any AI or GPT Tool privately licenced	No	Yes	No	No

Legend:

^ - AI tool is not commonly provided to all students; provisioning is dependent on Instructor's or Administrator's application.

* - Permission Required

- From Instructors if the AI Tool is used during course work.
- From School / Department Administrators if the AI Tool is used to support the administration of student services.

Appendix

SMU DATA CLASSIFICATION & SECURITY POLICY (STUDENTS)
Guidance on (i) Data Classification, (ii) Data Access, (iii) Data Transmission, (iv) Data Storage and (v) Disposal

Guidance	**Unrestricted (Low Risk)**	**Restricted** (Medium Risk) (Medium Protection)	**Sensitive** (High Risk) (High Protection)	**Highly Sensitive** (Highest Risk) (Highest Protection)
1. Guidelines for Classification of Data	Disclosure causes no harm to SMU.	Disclosure is likely to cause harm to SMU.	Disclosure is likely to cause **serious** harm to SMU.	Disclosure is likely to cause **very serious** harm to SMU. Or where large amount of "Sensitive" information (≥ 500 individual's records) escalates the risks to SMU.
2. Possible Impact of Unauthorized Disclosure / Data Loss	Disclosures are meant for public use.	Disclosure could: (a) Affect normal processes of SMU. (b) Embarrass SMU. (c) Undermine public and stakeholders' confidence in SMU.	Disclosure could: (a) Affect important processes of SMU. (b) Cause SMU to be punished by the Government or by law. (c) Affect SMU's position in negotiations. (d) Damage stakeholders' confidence in SMU.	Disclosure could: (a) Affect critical processes of SMU. (b) Cause severe punishment by the Government or by law. (c) Severely damage the public's confidence in SMU. (d) Severely damage SMU's international standing.
3. Types of Data	Approved public-facing marketing materials, messages, press releases, speeches.	Materials typically for internal use only. Internal emails on normal work matters.	NRIC/FIN & Passport numbers. Personnel files. Exam/test questions before exams.	SMU confidential papers. Any list of data ≥ 500 records containing personal data, health records, etc.
4. Transmission of Data	(a) Protection as desired. (b) SMU email to be used.	(a) Protection (passwords or encryption tool) where necessary. (b) SMU email to be used.	(a) Protection (passwords or encryption tool) is required. (b) SMU email to be used.	(a) Protection is **mandatory**. (b) SMU email to be used. (c) No social media or webmail allowed.

Guidance	**Unrestricted** **(Low Risk)**	**Restricted** (Medium Risk) (Medium Protection)	**Sensitive** (High Risk) (High Protection)	**Highly Sensitive** (Highest Risk) (Highest Protection)
6. Storage of Data	Care should be taken to protect integrity of information.	Protection where necessary (user's operational discretion).	(a) Protection is required. (b) Restrictions on equipment or devices or SMU storage.	(a) Protection is **mandatory**. (b) Only on **approved** equipment or devices or SMU storage.
7. Data Disposal	(a) Deleting files or reformatting digital storage devices.	(b) Reuse digital storage devices only after reformatting (c) Shred hard copies.	(a) Reuse digital storage devices only after reformatting (b) Shred hard copies finely.	(a) Destruct digital storages beyond recovery. Seek assistance from IT Help Centre (Tel: 6828 0123 or Email: helpdesk@smu.edu.sg) if required. (b) Shred hard copies finely.