Charles Sturt University

S E C U R E GenAI use framework for staff

For further information please contact

Associate Professor Mark A. Bassett
Director, Academic Quality and Standards
Academic Lead (Artificial Intelligence)
Deputy Vice-chancellor (Academic) Portfolio
Charles Sturt University

Charles Sturt University - TEQSA Provider Identification: PRV12018 (Australian University). CRICOS Provider: 00005F

S E C U R E

GenAI use framework for staff

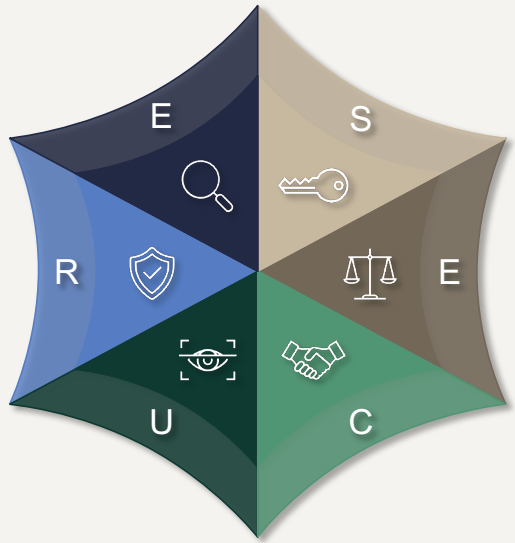
Charles Sturt University

Overview

The S.E.C.U.R.E. framework provides staff with clear, practical guidance for the responsible use of GenAI tools within defined risk parameters without requiring explicit University approval for low-risk activities.

It organises GenAI-related risks into six categories:

1. Security credentials
2. Ethical use
3. Confidential information
4. Use of personal information
5. Rights protection, and
6. Evaluation of outputs



The framework supports staff in experimenting safely with GenAI while safeguarding sensitive data, upholding university standards, and maintaining ethical integrity.

Risk categories

S E C U R E

GenAI use framework for staff

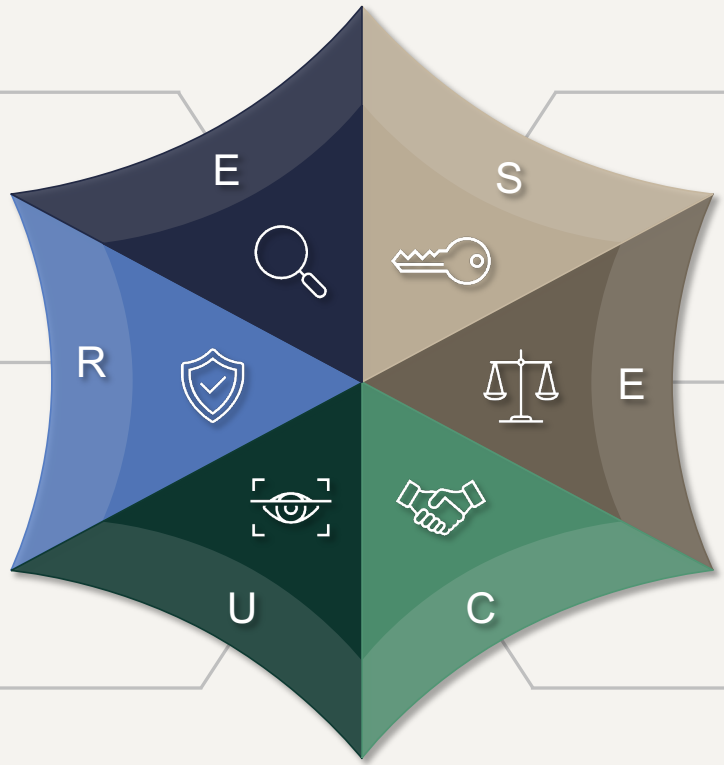
Charles Sturt University

6 EVALUATION OF OUTPUTS

Ensures the output is not used without being critically reviewed for accuracy and quality by staff.

1 SECURITY CREDENTIALS

Covers the handling of login details, passwords, API keys, and other security-related credentials.



5 RIGHTS PROTECTION

Protects the rights of creators of original works from unauthorised use.

2 ETHICAL USE

Entering or producing information that raises ethical issues, particularly involving First Nations Peoples' cultural knowledge, and the ethical use of the output of GenAI.

4 USE OF PERSONAL INFORMATION

Focuses on the use of personal, sensitive, or traceable information.

3 CONFIDENTIAL INFORMATION

Concerns data vital to the university's financial or competitive position.

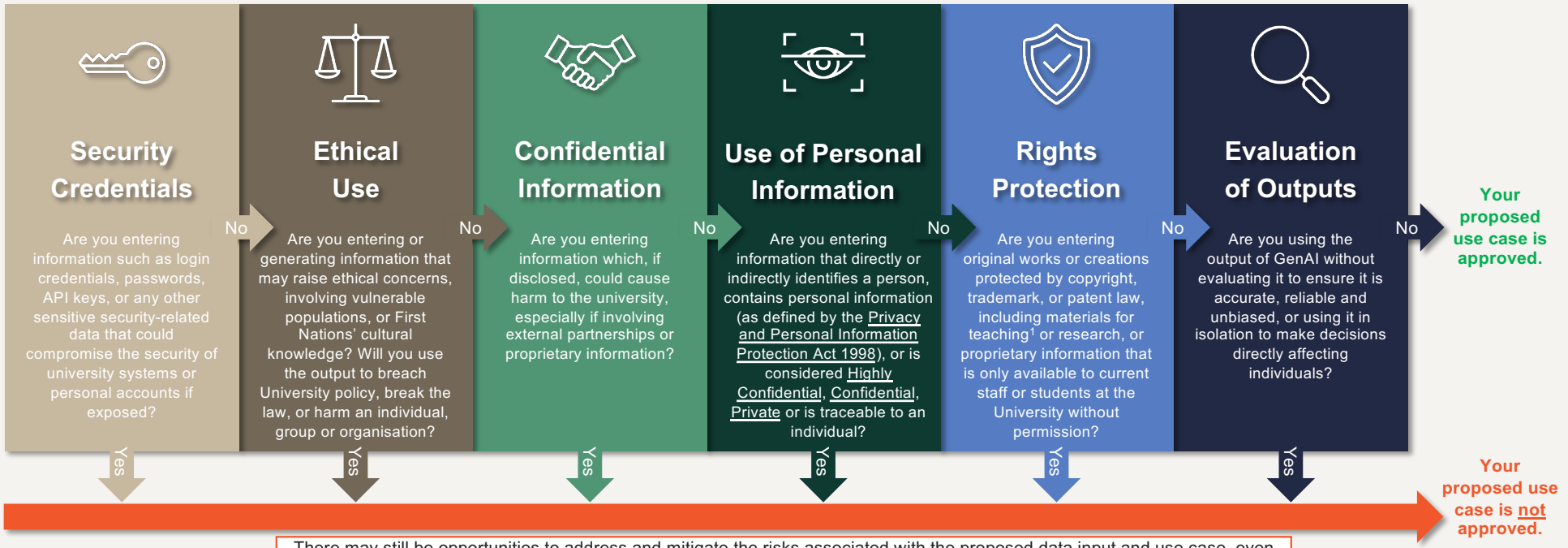
Charles Sturt University is an Australian University, TEQSA Provider Identification: PRV12018.
Charles Sturt University CRICOS Provider Number: 00005F.

Use case approval

S E C U R E

GenAI use framework for staff

Charles Sturt University



There may still be opportunities to address and mitigate the risks associated with the proposed data input and use case, even if they fall outside the S.E.C.U.R.E. framework. When a 'Yes' response occurs, staff should follow the steps outlined below.

[1] *Staff are permitted to input lecture slides/notes, teaching materials, Subject Outlines and publicly available university materials into GenAI software. Staff are not permitted to connect third-party software, including GenAI tools, to University systems without explicit approval from DIT.*

Risk category examples

S E C U R E

GenAI use framework for staff

Charles Sturt University

Security Credentials

University system login credentials (e.g. email passwords, LMS login details). API keys used for accessing external services. Private security tokens or encryption keys. Any credentials used to access internal systems.

Ethical Use

Data from vulnerable groups Entering or generating First Nations' cultural knowledge. Experimental or high-risk research data. Using the output to harass, harm, intimidate, breach policy or break the law.

Confidential Information

Unpublished research with commercial applications. Contracts or agreements with external partners. Financial data or sensitive strategic plans. Business development plans.

Use of Personal Information

Personal information: Names, student/staff IDs, emails, addresses. Sensitive data: Grades, health information. Traceable data: Personalised learning analytics reports or logs of student participation.

Rights Protection

Research publications, unpublished research, manuscripts, and theses. Creative works like software, art, books, music compositions. Textbooks, protected works. Student assessments.

Evaluation of Outputs

Using content from GenAI without verifying its accuracy. Submitting AI-generated text as an official University communication without checking for errors, inconsistencies, or misrepresentations. Relying on GenAI output alone to make a decision.

When SECURE flags a risk

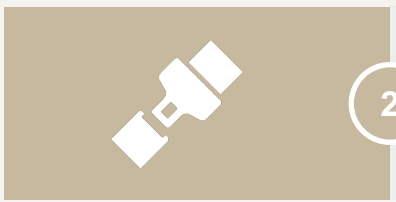
SECURE
GenAI use framework for staff

Charles Sturt University

1

Pause and evaluate

Determine which category within the S.E.C.U.R.E. framework triggered the 'YES' response. This helps identify the specific risk (e.g., security credentials, personally identifiable information, confidential information, etc.).



2

Mitigate identified risks

Assess whether safeguards or alternative approaches can mitigate the identified risk.
E.g., Anonymise data, quality-assure the output or change how the output will be used.

3

Seek approval

If risks cannot be mitigated, staff must escalate the situation by

a) Emailing the Division of Information Technology (DIT).

b) Providing a detailed description of the intended use case, including:
   - The specific data to be input
   - The purpose and expected output of GenAI
   - The proposed risk mitigation measures

c) Awaiting explicit approval or guidance from DIT.

Approval responses

S E C U R E
GenAI use framework for staff

Charles Sturt University

Proceed

If DIT confirms that the proposed data input and use case presents no risk, staff can proceed with the planned use case.

Proceed with caution or modify use case

- Implement any additional safeguards recommended.
- Adjust the proposed use case to align with university policies and the S.E.C.U.R.E. framework.
- Monitor usage to ensure continued compliance with safeguards.

Do not proceed

- Refrain from using GenAI for the intended purpose.
- Seek alternative methods that comply with the S.E.C.U.R.E. framework and university policies.
- Consider consulting with relevant teams, such as legal or data privacy officers, for further advice.

4

Document the process

- The identified risks and steps taken to mitigate them
- Any communications with DIT.
- Any approvals or recommendations received.