# TRU AI Use & Governance Guidelines

## 1. Purpose & Scope

These guidelines establish a unified, institution-wide framework for safe, ethical, equitable, and effective use of Artificial Intelligence (AI) at TRU. They apply to **students, faculty, staff, and researchers**, with additional role-specific expectations.

**Goals:**

- Support the TRU community on the foundational thinking of AI.
- Enable confident action by the TRU community.
- Build practical judgment for the TRU community.
- Encourage learning, experimentation, and escalation in a responsible manner.
- Protect privacy, security, academic integrity, and institutional trust.
- Provide a foundation for future **role-specific sub-guidelines**.

## 2. Guiding Principles

- **Human accountability** – Users remain responsible for decisions and outputs.
- **Privacy first** – Protect personal and confidential information.
- **Transparency** – Disclose meaningful AI involvement where required.
- **Equity & inclusion** – Reduce barriers and mitigate bias.
- **Security by design** – Use TRU-approved tools and follow information-security best practices.
- **Continuous improvement** – Review guidelines annually or when laws or technologies change.
- **Align with TRU policies** – FIPPA, academic integrity standards, research ethics, and cybersecurity practices.

## 3. Definitions

- **Personal information** is information about an individual who can be identified either from the information itself, or in combination with other available information. [FIPPA definitions]

    - **Any** student information is personal information, including the fact that an individual is a TRU student.
    - **Business contact information** (name, title, work phone/email) is not personal information.

- **Non-sensitive data** refers to information that cannot be used to identify an individual, either on its own or in combination with other data. This includes general, anonymized, or aggregated content that does not contain personal identifiers.
    - **Examples of non-sensitive data** include meeting agendas without names, generic templates, anonymized survey results, and content that excludes personal details.
    - **Personally identifiable data** is not considered non-sensitive and must not be used in AI processes unless permitted and protected.

## 3A. Use-Case Risk Classification

TRU recognizes that some AI applications pose higher risks due to their impact on individuals or institutional outcomes, regardless of underlying data sensitivity. All AI uses must be classified according to risk:

- **High-Impact Use Cases:** Includes grading, admissions decisions, hiring, performance evaluation, disciplinary actions, and allocation of financial aid. These uses require explicit risk flagging and additional oversight.
- **Moderate-Impact Use Cases:** Includes workflow automation, administrative efficiency, scheduling, or general research assistance. Oversight is required but less stringent.
- **Low-Impact Use Cases:** Includes drafting, brainstorming, and accessibility support with non-sensitive data.

All high-impact AI applications must be reviewed by the appropriate department or committee prior to deployment. Periodic audits are required to ensure ongoing compliance and mitigate risk.

## 4. Tool Approval, IT Security & Responsible Use

- Use only TRU-approved AI platforms (Copilot) or submit a PIA for any work involving sensitive or personal information.
- Do not share or store credentials in AI tools.
- Avoid personal accounts or consumer services for TRU business.
- Follow TRU IT Security guidelines, including remote-work safeguards.

## 4A. Prohibited AI Practices

To maintain ethical standards and protect institutional integrity, the following AI practices are strictly prohibited at TRU:

- AI-driven decision-making in grading, admissions, hiring, or disciplinary processes without human review and oversight.
- Use of AI for surveillance, monitoring, or profiling of individuals, including students, employees, or visitors.
- Deployment of AI systems that intentionally mislead, manipulate, or discriminate against individuals or groups.
- Use of AI to generate or propagate misinformation, deepfakes, or fraudulent content.
- Automated processing of sensitive or privileged information in non-approved tools, even if anonymized.
- AI applications that infringe on legal rights, privacy, or academic freedom.
- Any use of banned or blacklisted AI tools as determined by TRU or regulatory authorities.

## 5. Transparency, Accuracy & Academic Integrity

- Disclose meaningful AI use as required by instructors, departments, or publishers.
- AI must **not** be listed as an author.
- Students must follow assignment-specific rules.
- Cite AI tools appropriately when required.

Academic integrity violations include:

- Using fabricated or AI-generated sources.
- Submitting AI-generated work as original work when not allowed.
- Misrepresenting AI contributions.
- Falsifying data or research outputs.

## 5A. Equity Impact Check for High-Risk AI Uses

For any high-impact AI use-case (as defined in section 3A), TRU requires a lightweight equity impact check prior to deployment:

1. Identify potential impacts on equity, inclusion, and individual rights.
2. Consult relevant stakeholders, including affected groups and subject matter experts.
3. Document mitigation strategies for identified risks and develop a summary for transparency.
4. Review and update the equity impact check annually or after significant changes to the AI system.

The equity impact check should be concise and integrated into project planning, ensuring that higher-risk AI uses do not reinforce bias or create unfair outcomes.

## 6. Judgment & Oversight Requirements

All AI users must:

- Verify facts, citations, formulas, and code before use.
- Detect and correct hallucinations, bias, or inaccuracies.
- Avoid over-reliance on AI.
- Ensure compliance with TRU policies (Academic Integrity, FIPPA, Research Ethics, IT Security).
- Maintain full responsibility for submitted or published work.

## 7. Data Governance & Privacy Requirements

**Do NOT enter this information into non-approved AI tools:**

- Personal information (e.g. assessment content, student names/numbers, addresses)

- Privileged information
- Grades, evaluations, HR materials, hiring documents.
- Unpublished, sensitive, or identifiable research data.
- Internal financial or planning documents.
- Assessment content (exam banks, quiz items).
- Credentials, security configurations, or restricted IT information.

**TRU Data Classification**

- **Public:** Data designed for unrestricted public viewing, such as released research findings, course listings, or event notifications. This type of information can be freely distributed without causing harm to any person or to TRU.
- **Internal:** This information is for internal university use; unauthorized sharing could disrupt operations or harm TRU's reputation.
- **Confidential:** Confidential university data intended solely for authorized users. Exposure or misuse of this information can result in damage to the institution's reputation, breach of legal obligations, or violation of university policies. Examples include, but not limited to:
    - Academic records, including grades, transcripts, and student identification numbers.
    - Personnel documents such as faculty evaluations and tenure review materials.
    - Internal financial statements and budget planning documents.
    - Unpublished research data generated within the university.
    - Legal agreements, contracts, and related documentation.
    - Grant applications and proposals not yet released to the public.
    - Personal information as defined in Freedom of Information and Protection of Privacy Act (FIPPA).
    - Privileged Information
    - De-identified content that cannot reasonably identify individuals or institutional processes.

**FIPPA Compliance**

- As a BC public institution, TRU must ensure personal data is not stored or processed outside Canada unless permitted under FIPPA.

- TRU must only collect, use, and disclose personal information as set out in FIPPA. When entering personal information into an AI tool, ensure this use is consistent with the purpose for which the information was collected.
    - This means personal information is either being used for the same purpose it was originally collected, or for a purpose that has a reasonable and direct connection to the original purpose, and that is necessary for a TRU program or activity.

## 8. Encouraged & Acceptable Uses

AI tools may be used to support creativity, learning, productivity, and accessibility **provided no restricted data is used**.

**General Acceptable Uses**

- Drafting, editing, outlining, and summarizing **non-sensitive data**.
- Brainstorming, ideation, alternative phrasing.
- Accessibility support (plain language, alt-text, captions, alternative formats).
- Administrative efficiency (templates, checklists, meeting notes).
- Coding assistance and workflow automation.
- Non-sensitive research assistance (e.g., summaries, structure generation).

**Roles:**

- **Students:** Follow course-level AI expectations. Use AI ethically for brainstorming, outlining, and study support unless prohibited by instructors. Enhance learning with explanation or practice questions. Evaluate AI output critically. Disclose AI use when required.
- **Faculty:** Clearly communicate AI rules in syllabi. Draft communications, teaching materials, job aids, and examples using AI, but protect student data and personal information. Only enter confidential data (including personal information) into approved tools. Ensure assessments maintain academic integrity. Develop alternative formats and accessibility-support resources with AI.
- **Staff:** Use AI for administrative tasks such as templates, checklists, and meeting notes. Only enter confidential data (including personal information) into approved tools. Support peers through training and safe practice.

- **Researchers:** Use AI for non-sensitive ideation, literature scaffolds, or coding assistance. Obtain REB approval before processing private or sensitive data. Document AI use transparently. Disclose AI involvement in publications as required. Follow TCPS2, FIPPA, and TRU research policy.

## 9. Equity, Inclusion & Accessibility

AI use should:

- Reduce barriers through simplified language, multimodal output, and alternative formats.
- Avoid reinforcement of stereotypes or bias.
- Support, not replace, required human accommodations.
- Promote accessible learning environments.

High-impact AI use cases must complete the equity impact check described in Section 5A before deployment. Results should be documented and available for review.

## 10. Escalation & Reporting

- **Privacy concerns or breaches** – TRU Privacy & Access Office, Information Security. See the TRU Breach Protocol.
- **Security or IT issues** – ITS Service Desk.
- **Research Ethics Questions** – Research Ethics Board / Research Services.
- **Library support** – TRU Library for citation, evaluation, and technology guidance.
- **Policy guidance** – Department heads or the TRU Policy Office.

All reports involving prohibited AI practices or equity concerns must be escalated to the relevant oversight body for review and remediation.

## 11. Key Learning Resources

- TRU AI Education Hub [GenAI in Education]
- TRU AI Guidance for Educators [Guidance – GenAI in Education]

- TRU AI Hub for Employees [AI for Employees]
- TRU Library AI Guides (appropriate uses, evaluating output) [TRU Library – AI Guide]
- TRU Academic Integrity Policies [Centre for Academic Integrity, Academic Integrity - Case Process]
- FIPPA (BC Privacy Legislation applicable to TRU) [FIPPA]
- OIPC BC AI & Privacy Guidance [Guidance Documents – IOPC BC]

## 12. Governance & Review

- Owned by **Teaching** & Learning + Research Office and ITS.
- Reviewed **annually** or after significant policy or legislative changes.
- Workgroups may develop **role-specific sub-guidelines**.

## 13. Disclaimer

These guidelines support, but do not replace, official TRU policies, research ethics requirements, or provincial/federal privacy legislation. In cases of conflict, **TRU** Policy Index and **FIPPA** take precedence.

## Acronyms & Full Forms

- **AI** – Artificial Intelligence
- **FIPPA** – Freedom of Information and Protection of Privacy Act (BC)
- **ITS** – Information Technology Services
- **REB** – Research Ethics Board
- **PIA** – Privacy Impact Assessment
- **TCPS2** – Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans
- **TRU** – Thompson Rivers University
- More Terms – AI Glossary Terms – AI for Employees