CR603: Artificial Intelligence (AI) Corporate Policy

Policy Title:	Artificial Intelligence (AI) Corporate Policy
Policy Number:	CR 603
Owner:	Chief Information Officer
Approved by:	Corporate Policy Panel and SLT
Effective Date:	May 2026
Reference:	
Links to Other Policy:	AC517: Artificial Intelligence (AI) in The Classroom

St. Lawrence College is committed to making our resources fully accessible to all persons. This document will be made available in alternative format upon request.

BACKGROUND

Definitions:

For the purposes of this policy, Artificial Intelligence (AI) refers to computer systems or software that perform tasks that typically require human intelligence, such as generating content, analyzing data, identifying patterns, making predictions, or supporting decision-making. This definition is functional rather than technical and is intended to support a shared understanding across the SLC community.

Types of AI Systems: AI systems may include the following categories:

1. **Generative AI:** Tools that create new content such as text, images, audio, video, or code.
2. **Predictive & Analytical AI:** Systems that analyze data to forecast outcomes/trends.
3. **Machine Learning Systems** – Applications that adapt or improve performance over time based on data patterns.
4. **AI-enabled tools embedded in software** – AI capabilities integrated into commonly used platforms rather than standalone tools.
5. **Agentic AI** – AI systems that can initiate pre-approved actions, execute multi-step tasks, or interact with systems with limited real-time human input.

What is not AI: Not all automation or digital tools are considered AI. Rule-based systems, basic scripts, macros, or traditional software that does not learn, adapt, or generate outputs dynamically are not considered AI under this policy.

Purpose:

The purpose of this policy is to provide clear principles and governance guardrails for the responsible, ethical, and secure use of Artificial Intelligence (AI) at St. Lawrence College (SLC). SLC recognizes the transformative potential of AI to enhance student experience, student learning, teaching, research, and administrative effectiveness. At the same time, AI introduces risks related to privacy, security, bias, accuracy, and academic integrity.

This policy seeks to enable innovation while managing risk in a thoughtful and proportionate manner. It establishes principles and expectations, not detailed technical or instructional requirements.

Scope:

This policy applies to all members of the St. Lawrence College community, including:

- Faculty
- Staff and administrators
- Students
- Contractors, consultants, and third parties acting on behalf of the College

This policy applies to the use of AI tools regardless of whether the tool is:

- Free or paid
- Institutionally approved or independently accessed
- Embedded within another software product or platform

Users remain accountable for decisions and actions taken when using AI systems in connection with SLC activities.

POLICY STATEMENTS

1. Human Accountability

Artificial Intelligence (AI) systems shall be used to support, not replace, human judgment. Individuals and organizational units remain accountable for decisions, actions, and outcomes resulting from the use of AI.

2. Academic Integrity

The use of AI in academic contexts shall uphold principles of academic integrity. AI shall not replace core learning, thinking, authorship, or assessment of student achievement. Expectations for AI use must be clearly communicated where applicable.

3. Privacy and Data Protection

AI shall be used in a manner that protects personal, confidential, and sensitive information. Such data shall not be entered into AI tools unless those tools have been institutionally approved for the specific data classification and use case.

4. Fairness and Ethical Use

AI shall not be used in ways that introduce bias, inequity, discrimination, or harm. Potential impacts on students, employees, and other members of the College community must be considered when deploying or using AI.

5. Transparency

Where AI meaningfully contributes to academic work, institutional communications, or decision-making processes, its use shall be transparent and not misleading. AI-generated or AI-assisted content must be subject to appropriate human review.

6. Security by Default

AI shall be implemented and used in alignment with the College's security, risk management, and operational standards. AI tools must not be connected to institutional systems or data without appropriate technical review and authorization.

MONITORING

Oversight of this policy is the responsibility of the Chief Information Officer (CIO). The effectiveness of this policy will be monitored through:

- Ongoing review of AI use across academic, administrative, and operational contexts
- Identification of emerging risks, issues, or unintended impacts
- Feedback from academic leadership, service owners, and institutional governance bodies
- Alignment with changes in legislation, regulation, or institutional risk profile

Findings from monitoring activities may inform updates to this policy, related procedures, or supporting guidance as required.

NEXT POLICY REVISION DATE

May 2027 (Early review due to emerging technology)

SPECIFIC LINKS

- Academic Integrity Policy
- Acceptable Use Policy for Technology Services (CR 601)
- Privacy and Information Management policies
- Vulnerability Management Policy (CR 604)
- Data Governance and Data Retention policies
- Procurement and Vendor Management policies

APPENDIX A AND ATTACHMENTS

Appendix A - A Practical decision guide for SLC Leaders & Faculty

This guide helps you apply the College's AI principles when deciding **whether and how** to use AI in academic, administrative, or operational contexts. If you are unsure whether a specific AI use is appropriate, walk through the questions below.

Question 1: What role is AI playing?

- Is AI supporting my thinking, drafting, analysis, or planning?
- Or is AI being asked to make or replace a human decision?

Appropriate: AI assists with drafting, summarizing, brainstorming, analysis, or pattern recognition

Not appropriate: AI makes final decisions about students, employees, grades, admissions, or evaluations without human in the loop.

Principle applied: Human Accountability

Question 2: Does this Use Case support Student Learning and Academic integrity?

- Does this AI Use Case align with the learning outcomes or intent of the activity?
- Would a reasonable person still see this work as demonstrating the student's own learning?

Appropriate: AI supports learning, exploration, feedback, or skill development

Not appropriate: AI replaces the core learning, thinking, or authorship the activity is meant to assess

Tip for faculty: If expectations are unclear, **state explicitly** how AI may or may not be used in the course or assignment.

Principle applied: Academic Integrity

Question 3: What data is being shared with the AI tool?

- Am I entering personal, confidential, or sensitive data?
- Do I know where this data goes, how it is stored, or how it may be reused?

Appropriate: Public, low-risk, or anonymized information in approved tools

Not appropriate: Student records, grades, employee data, health, financial, or confidential institutional information in unapproved tools.

Principle applied: Privacy & Data Protection

Question 4: Could this AI use introduce bias, unfairness, or harm?

- Could this AI output disadvantage certain individuals or groups?
- Am I relying on AI recommendations without questioning assumptions or limitations?

Appropriate: AI insights are reviewed critically and contextualized

Not appropriate: AI outputs are accepted uncritically, used in ways that discriminate or mislead.

Principle applied: Fairness & Ethics

Question 5: Is the use of AI transparent where it matters?

- Would others reasonably expect to know that AI was used?
- Could someone be misled about authorship or decision-making?

Appropriate: AI use is disclosed where it meaningfully affects work, assessment, or communication

Not appropriate: AI use is hidden in ways that undermine trust or accountability

Principle applied: Transparency

Question 6: Is this tool appropriate from a security and risk perspective?

- Is this an approved or institutionally supported tool?
- Does this use introduce security or operational risk?

Appropriate: AI tool has been reviewed and is aligned with existing IT, security, and risk practices

Not appropriate: Convenience overrides security, or risks cannot be reasonably mitigated

Principle applied: Security by Default

Appendix B – Illustrative Examples of AI Use

This appendix provides illustrative examples to support understanding of how the Artificial Intelligence (AI) Policy may be applied in practice.

The examples below are not exhaustive and do not replace professional judgment. Specific use cases should always be assessed using *Appendix A – Practical AI Decision Guide.*

B.1 Illustrative Acceptable Uses of AI (with Conditions)

The following examples generally align with this policy when used with appropriate human oversight, disclosure where required, and compliance with privacy, security, and academic integrity requirements:

- Drafting emails, reports, briefing notes, policies, or presentations with human review and validation
- Summarizing documents, meeting notes, or large volumes of information
- Brainstorming ideas, exploring alternative approaches, or supporting creative and analytical thinking
- Using AI as a tutoring or learning aid to explain concepts or provide practice material, where aligned with course expectations
- Supporting administrative efficiency tasks such as formatting documents, organizing information, or preparing first drafts
- Assisting with early-stage research exploration, coding support, or data analysis, subject to research ethics and data governance requirements

B.2 Illustrative Prohibited Uses of AI

The following examples are not permitted under this policy:

- Entering personal, confidential, sensitive, or regulated data (e.g., student records, grades, employee data, health or financial information) into unapproved AI tools
- Using AI to make fully automated decisions about admissions, grading, hiring, performance management, or disciplinary actions without meaningful human oversight
- Presenting AI-generated or AI-assisted content as fully human-created where transparency or disclosure would reasonably be expected
- Using AI in ways that conflict with existing College policies, including academic integrity, privacy, cybersecurity, or acceptable use policies
- Connecting AI tools to institutional systems or data sources without appropriate review and authorization

B.3 Important Note

These examples are intended to clarify policy intent, not to create additional rules or approvals.
As AI technologies and use cases evolve, these examples may be updated without requiring formal policy revision.