Artificial Intelligence Accountability Framework

History and Context

In June 2023, the OASBO Joint Collaborative Committee initiated discussions on the use of Generative AI tools and established a working group to explore related issues. By spring 2024, two distinct work streams were formed: one focused on developing Guidelines for the Responsible Use of Generative AI, and the other on compiling Generative AI Resources. These documents were designed to support school boards, with particular emphasis on educator use.

During the 2024–2025 school year, both documents were finalized and distributed across the province. In fall 2025, the working group was renewed, expanding to over 130 members representing a wide range of educational roles throughout Ontario. A dedicated sub-group of drafters and reviewers was tasked with creating the Artificial Intelligence Accountability Framework document, which was subsequently reviewed by the full working group and submitted to ECNO and OASBO for final approval.

This document is intended as a starting point for Ontario School Boards, and it is intended to be copied, reviewed, and modified for your board's specific and unique circumstances.

Generative AI continues to develop rapidly, and thus these documents must be read in the context of our collective understanding at the point in time of publication.

Framework Statement

The [School Board Name] recognizes the transformative potential of Artificial Intelligence (AI) to enhance educational and operational outcomes. We are committed to mitigating risks by prioritizing student and staff privacy, promoting equity, and upholding human oversight. This framework establishes comprehensive governance structures to guide the responsible integration and utilization of AI technologies across our educational system.

The framework recognizes that Artificial Intelligence will inevitably become part of both central corporate operations and school-based administrative tasks, making it essential to establish clear parameters now that protect sensitive information, ensure compliance with privacy legislation like Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and integrates requirements under Ontario's Bill 194 Enhancing Digital Security and Trust Act (EDSTA), best practices from industry security standards, as well as following required accommodations under human rights law. This will ensure our AI initiatives serve our core mission of student success while maintaining the highest standards of safety, transparency, and accountability.

Purpose and Scope

Purpose: To provide clear guidance for all board staff on the appropriate use of AI technologies in our organization while establishing governance structures that ensure responsible innovation, and to recognize and respect the specific AI-related professional standards, ethics, and regulatory expectations applicable to regulated staff.

Scope: This framework applies to all AI tools and systems used within the board, including but not limited to:

- Generative AI tools (text, image, audio, video generation)
- Learning management system AI features
- Administrative automation systems
- Student information system AI components
- Third-party educational technology with AI capabilities
- AI-powered assessment and grading tools
- AI-driven workflow and resource management tools
- Agentic AI Systems AI tools capable of autonomous decision-making, complex goal execution, and operating without continuous human intervention.

Guiding Principles

Our approach to AI governance is guided by eight foundational principles:

1. Human-Centered Focus

All AI implementations must demonstrably benefit student and staff learning, student and staff well-being and educational outcomes while preserving and enhancing human connection and personalized instruction.

2. Operational Effectiveness

AI implementations must demonstrate administrative efficiency, accuracy, and service quality while preserving human oversight.

3. Privacy and Data Protection

AI systems must comply with existing board procedures, all applicable privacy legislation, and maintain the highest standards for protecting student and staff personal information.

4. Equity and Accessibility

All approved AI tools and their benefits must be accessible to all students and staff, factoring in age-based privacy compliance, and staff, with particular attention to avoiding bias and ensuring inclusive design.

5. Transparency and Explainability

The use of AI in educational and administrative decisions must be transparent to affected stakeholders, with clear explanations of how AI systems inform decision-making.

6. Human Oversight and Agency

All staff retain ultimate responsibility for educational and operational decisions, with AI serving as a tool to support rather than replace human judgment.

7. Continuous Learning and Improvement

Our approach to AI will evolve based on research, experience, and changing technology, with regular evaluation and adaptation of policies and practices.

8. Responsible Innovation

We will thoughtfully evaluate new AI technologies, prioritizing student achievement, student and staff wellbeing, and privacy and security over rapid adoption.

Governance Structure

AI Governance Committee

The purpose of the AI Governance Committee is to provide strategic oversight, direction, and risk mitigation concerning the implementation and use of Artificial Intelligence technologies across the board. The committee acts as an advisory and integrating mechanism, ensuring that AI adoption aligns with the board's goals, and ethical commitments, particularly in the areas of privacy, data security, equity, and regulatory compliance.

Membership may include:

- Director and/or Superintendent
- CIO/Senior IT Manager
- CISO
- Privacy Officer
- System Level Principal
- Program Consultants
- Principal Representative
- Teacher Representative
- Student Representative (secondary)
- Union and Labour Partners
- Caregiver Representatives

Responsibilities may include:

- Remaining current on legislation and technological changes and/or advancements
- Oversee framework implementation and compliance
- Review transparency and community engagement
- Review of educational impact and effectiveness
- Review professional development initiatives and opportunities

AI System Classification and Risk Management

Risk Classification Framework (Flowchart included in Appendix)

Requires full governance review and ongoing monitoring

HIGH RISK - Requires full governance review and ongoing monitoring

- AI systems that directly impact student grades, placement, or disciplinary actions
- AI systems processing sensitive personal data, impacting HR decisions, financial transactions, or legal compliance.
- AI tools processing sensitive student health or behavioral data
- Systems using predictive analytics for student outcomes

Recommended Governance Steps:

- Conduct a comprehensive risk assessment (privacy, bias, security, impact).
- Obtain approval from the AI governance committee.
- Ensure compliance with legal and regulatory requirements (MFIPPA, PHIPA, Education Act, Enhancing Digital Security and Trust Act).
- Implement robust data protection and privacy safeguards.
- Establish clear documentation and audit trails.
- Provide professional growth opportunities for responsible use and oversight.
- Set up ongoing monitoring and annual re-evaluation.
- Follow existing board incident response and reporting protocols.

MODERATE RISK - Requires governance committee and departmental review and periodic monitoring

- Learning management systems (i.e. Brightspace) AI features
- AI-powered tutoring and instructional support tools
- Workflow automation, communications, scheduling, and resource management.
- Requires departmental review and periodic monitoring

Recommended Governance Steps:

- Perform a departmental risk assessment (focus on data use, fairness, and transparency).
- Obtain approval from the AI governance board.
- Document intended use, data flows, and user access.
- Support capacity building for staff in the effective use of digital tools.

LOW RISK - Departmental approval with annual review

- General productivity tools (document creation, scheduling)
- Basic research and information gathering tools

- Simple chatbots for general school information
- Non-personalized content generation tools
- Departmental approval with annual review

Recommended Governance Steps:

- Complete a simple risk checklist (data privacy, intended use).
- Obtain sign-off from Principal or Manager.
- Maintain a record of tools in use.
- Review tool usage and risks annually.
- Support capacity building for staff in the effective use of digital tools

Risk Assessment Process (applies to all levels):

1. Identify the purpose and scope of the AI tool.
2. Assess data sensitivity and potential impact on students/staff.
3. Evaluate transparency, explainability, and fairness.
4. Determine compliance with institutional and legal standards.
5. Document findings and recommended actions.

END: Implement the AI Tool According to Governance Steps

Risk Assessment Process

All AI systems must undergo evaluation using the standardized assessment framework:

1. **Operational Value Assessment**
    a. Clear articulation of operational benefits (e.g., improved efficiency, accuracy, cost savings, service quality).
    b. Alignment with school board strategic and operational goals (e.g., compliance, resource management, stakeholder service).
    c. Evidence of effectiveness from research, case studies, or pilot programs relevant to administrative functions.
2. **Privacy Impact Assessment (PIA)**
    a. Data collection and processing analysis
    b. Consent and notification requirements
    c. Data retention and deletion procedures
    d. Third-party data sharing agreements
3. **Bias and Equity Review**
    a. Analysis of potential discriminatory impacts
    b. Alignment with school board strategic and operational goals (e.g., compliance, resource management, stakeholder service)

c. Community input on equity considerations

4. **Security and Technical Review**
    a. Cybersecurity assessment
    b. Integration with existing systems
    c. Vendor security standards evaluation
    d. Incident response procedures
5. **Legal and Compliance Review**
    a. MFIPPA, PHIPA, Education Act, and Bill 194 EDSTA compliance verification
    b. Contractual terms and conditions review
    c. Vendor and 3rd party affiliates security standards evaluation

Implementation Guidelines

Approved Uses:

- Supporting operational planning, framework and resource development (with appropriate human oversight)
- Creating customized materials for communications, professional growth opportunities or administrative purposes
- Professional development planning
- Conducting research and supporting professional development for staff
- Automating administrative tasks (such as scheduling, communications, reporting, and workflow management)
- Accessibility (supports accessible learning, i.e. assistive technologies like speech to text, captioning, translation, etc.)
- Cybersecurity and threat detection for real-time anomaly detection, threat intelligence, automated incident response, and continuous monitoring to safeguard board data, systems, and networks.

Prohibited Uses:

- No Personally Identifiable Information (PII) or Board Intellectual Property (IP) should be input, stored, or used in Public Large Language Models (LLMs) unless specifically approved and governed by the board's data security protocols.
- Uploading or using non-public and confidential documents into a Public LLM that violates board policies or legal requirements
- Making decisions on personnel, disciplinary, or financial matters
- Analyzing personal or sensitive data
- Replacing essential human judgment or interaction in board operations

Professional Responsibilities:

- Complete required [school board] AI literacy professional growth opportunities
- Model ethical and responsible AI use
- Ensure all approved AI systems and practices safeguard student and staff data and comply with legal requirements, specifically those mandated by MFIPPA, PHIPA, and EDSTA.
- AI outputs created must be reviewed for copyright, bias, and appropriateness

Vendor Management and Procurement

To protect students, staff, and data when using AI tools, all vendors must meet clear standards for privacy, security, fairness, and accessibility.

All approved AI technology vendors must provide:

- System documentation and transparency reports explaining how the tool works and how decisions are made.
- Evidence of bias testing and mitigation strategies, showing efforts to ensure fairness and inclusion for all users.
- Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA) results, identifying how personal information and system risks are managed.
- Proof of privacy and security certifications, such as SOC 2 or ISO 27001.
- Clear data handling practices, including how data is collected, stored, shared, and deleted.
- Confirmation that outputs meet AODA accessibility standards, ensuring equitable access for all staff and students.
- Regular independent (third-party) security and compliance reviews.
- A risk management system that is established and implemented, which includes regular assessments intended to identify risks to Personal Information, and which promptly remediates such risks

Contract Provisions must include:

- The right to audit AI algorithms and data practices.
- Data portability and deletion guarantee, ensuring data can be moved or erased when needed.
- Defined liability and indemnification terms to protect the board from vendor errors or misuse.
- Ongoing reporting requirements, including updates on performance, bias, and accessibility compliance.
- Clear offboarding procedures, including data return, transfer, and certificate of destruction once the contract ends.

- Should include comprehensive Data Privacy Agreements (DPA), with particular attention to stipulations regarding data portability and the guarantee of deletion.

Professional Development

Essential Professional Learning Considerations

- Cyber security awareness, privacy management and incident reporting procedures
- Digital Literacy and online safety
- Board AI policies, Guidelines and Administrative Procedures
- Human Rights Impacts
- Accessibility and Inclusive Design
- Ethical considerations, equity and bias awareness
- Alignment with Professional Organization Standards (where applicable)
- Ongoing AI Awareness and/or Professional Development
- Regular updates on emerging AI technologies
- Best practices sharing and collaboration regarding prompt engineering
- Research-based implementation strategies
- Community of practice development
- Conference and professional development opportunities

Monitoring, Evaluation, and Continuous Improvement

Key Performance Indicator Considerations

Educational Impact:

- Student learning
- Teacher efficiency and satisfaction
- Equity of access
- Accessibility and inclusion
- Student engagement and well-being

Operational Effectiveness:

- **Corporate staff efficiency and satisfaction**
- System performance and reliability
- Value assessment
- User adoption and satisfaction rates

Compliance and Risk Management:

- Privacy breach incidents and response times
- Bias detection and mitigation effectiveness
- Privacy and Security Impact Assessments

Regular Review Processes

Annual Review:

- Evaluation of framework effectiveness
- Board community feedback integration (staff, students)
- Regulatory and legal requirement updates
- Best practice assessment
- Review Privacy and Security Impact Assessments
- Apps and licensing review

Quarterly Governance Review:

- AI system performance evaluation
- Risk assessment updates
- Incident analysis and improvement planning

Transparency and Community Engagement

Public Reporting Requirements

AI Transparency Report:

- Inventory of all AI systems in use
- Educational impact assessment results
- Privacy and security incident summary
- Community engagement activities summary
- Future AI planning and priorities
- Framework or procedure changes

Privacy Protection and Data Governance

Data Collection and Use Principles

Data Minimization: AI systems may only collect, process, and retain data that is necessary, relevant, and adequate for specified educational and operational purposes.

Purpose Limitation: Student and staff data used by AI systems must align with clearly defined educational and operational objectives.

Consent and Notice: Clear notification about AI data processing with appropriate consent mechanisms.

Data Quality: Regular verification of data accuracy and relevance for AI processing.

Student Privacy Protections

- Enhanced protections for students under 18
- Caregiver notification and consent procedures
- Student data portability and access rights
- Clear policies on AI-generated student records
- Regular privacy impact assessments
- Secure data transmission and storage protocols

Data Retention and Deletion

- Clear retention schedules for AI-processed data
- Automated deletion procedures where appropriate
- Regular data inventory and cleanup processes
- Vendor data return and deletion verification
- Documentation of data lifecycle management

Incident Response and Risk Mitigation

AI-Related Incident Categories

AI-related incidents are categorized into technical, educational, and privacy/legal & compliance areas, encompassing issues such as but not limited to:

Technical Problems

- These incidents involve the functional failure or operational degradation of AI systems and related infrastructure.
- Systems break down, run slowly, or stop working entirely.
- Hacking incidents or times when private data gets leaked due to technical vulnerabilities (also covered under Privacy/Legal).
- Interoperability failures where different applications or tools do not work together correctly.
- Service interruption when a third-party service provider (vendor) experiences a failure.
- Accessibility failures where AI systems or features create digital barriers or are otherwise non-functional for users with disabilities.

Equity & Educational Problems

- These incidents involve the fair and appropriate use of AI within the educational context, focusing on bias, conduct, and appropriate content.
- When an AI produces unfair, biased, or discriminatory outputs, impacting equity.
- Accessibility failures that result in non-compliance with standards like the Accessibility for Ontarians with Disabilities Act (AODA) or similar regulations.
- Misuse of AI for academic dishonesty, such as plagiarism or other forms of cheating.
- The AI creates offensive, harmful, or inappropriate content.
- Misuse of AI tools by students or staff in ways that violate policy (e.g., Code of Conduct, Appropriate Use).

Privacy, Legal & Compliance Problems

- These incidents involve unauthorized data access, policy breaches, and violations of external laws or contractual agreements.
- Unauthorized data access or use by someone without the required permission.
- The legal requirement to notify individuals that their private information was exposed (data breach notification).
- Violations of official rules, regulations, or laws (e.g., copyright, data protection laws).
- A third-party company (vendor) breaks its official agreement or contract with us.
- The use of unapproved applications or websites creates compliance risks.

All responses and mitigations must align with the board's Associated Response Plan, Policies, and Procedures.

Include links to templates: (Code of Conduct, Appropriate Use, BCP, IRP)

Legal and Regulatory Compliance

AI Usage will be governed by the following:

- Compliance with all legal and regulatory requirements
- A clear process for reviewing and vetting AI usage (Security and Privacy review)
- Comprehensive professional growth opportunities for staff and students
- Transparency of AI Usage

Future Considerations and Emerging Technologies

Technology Evolution Planning

- Regular environmental scanning for emerging AI technologies
- Research partnership development with educational institutions
- Pilot program framework for new AI tool evaluation
- Strategic planning integration for long-term AI vision

Framework Adaptation Framework

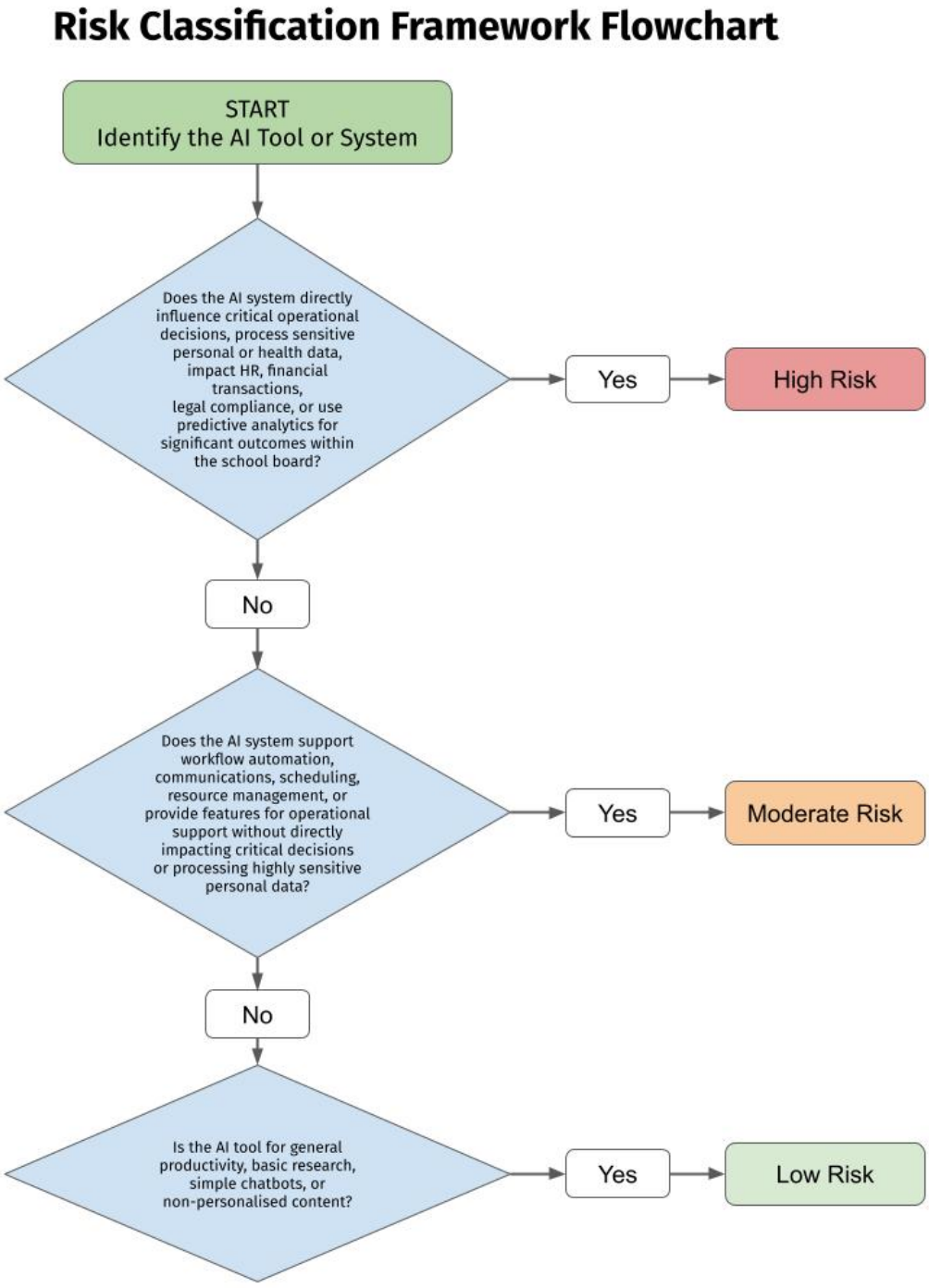
- Annual framework review and update procedures
- Stakeholder feedback integration mechanisms
- Best practice monitoring and implementation
- Regulatory change monitoring and compliance updates

Community Preparation

- Digital literacy curriculum development
- Caregiver and community education programs
- Ethical AI discussion and dialogue facilitation
- Future workforce preparation initiatives

Appendix

Editable version



Requirement	Low Risk	Moderate Risk	High Risk
Basic risk checklist (privacy, intended use)	✓	✓	✓
Central app approval team review and sign-off	✓	✓	✓

Governance committee review		✓	✓
Comprehensive risk assessment (privacy, bias, etc.)			✓
Alignment with board policies and regulations	✓	✓	✓
Privacy & security safeguards		✓	✓ (advanced)
Maintain usage logs and documentation	✓ (basic)	✓	✓ (detailed)
Staff professional growth opportunities		✓ (orientation)	✓ (formal)
Stakeholder engagement			✓
Audit trails			✓
Ongoing monitoring and annual re-evaluation	Annual	Semi-annual	Continuous

Resources

Professional Development Resources

- Copilot Prompt Gallery
- AI for Business Productivity
- Gemini Generative AI For Educators

Documentation and Citation

- How to Cite ChatGPT - APA Style
- How do I cite generative AI in MLA style?
- How do you recommend citing content developed or generated by artificial intelligence?

Ontario and Canada Privacy and AI Directives

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA): applies to municipal institutions and many Ontario school boards; sets rules on collection/use/disclosure and access.

Personal Health Information Protection Act (PHIPA): Ontario statute for handling personal health information (if you collect health/medical info about students/staff).

Ontario Responsible Use of Artificial Intelligence Directive: Provincial directive that sets transparency, accountability and risk management expectations for government AI use; useful as a baseline for public sector bodies in Ontario.

Canada Artificial Intelligence and Data Act (AIDA / AIDA companion): Canada's federal AI statute framework for risk-based regulation of certain AI systems and associated obligations.

Human Rights AI Impact Assessment: The purpose of the human rights AI impact assessments is to assist developers and administrators of AI systems to identify, assess, minimize or avoid discrimination and uphold human rights obligations throughout the lifecycle of an AI system.

Glossary

Artificial Intelligence (AI): AI refers to the capability of computers or algorithms to mimic intelligent human behavior, such as reasoning, learning, and problem-solving. It encompasses a broad field within computer science, focused on developing intelligent machines that can perform tasks that typically require human intelligence.

Bias in AI: This involves the tendency of AI systems to produce prejudiced outcomes due to the data they are trained on or the way they are programmed. Bias in AI can lead to unfair or unethical results, reflecting existing human prejudices in their outputs.

Catholic Social Teachings: A set of doctrines developed by the Catholic Church, emphasizing social justice, the dignity of human life, and the need for societal structures that support the common good. These teachings advocate for addressing poverty, inequality, and upholding human rights.

Copyright: A legal right granted to the creator of original works, including the exclusive right to reproduce, distribute, and display their work. Copyright laws aim to protect creators' intellectual property and encourage the creation of new works.

Data Privacy: Refers to the handling of sensitive information, especially personal data, in a way that respects individual privacy and confidentiality. It involves protecting data from unauthorized access, collection, use, or disclosure, and ensuring ethical use of personal information.

Digital Citizenship: The responsible use of technology by citizens involves the understanding of how to use technology ethically, legally, and safely. It includes awareness of one's digital footprint and the impact of digital actions on oneself and others.

Digital Literacy: The ability to use digital technology, communication tools, or networks to access, manage, integrate, evaluate, and create information. It involves the skill to use information ethically and effectively.

Ethical Use: In the context of technology and GenAI, ethical use refers to using these tools in a morally sound way, respects individual rights, and does not cause harm. This includes considering the impact of technology on privacy, security, and societal norms.

Generative Artificial Intelligence (GenAI): A type of AI that can generate new content or data based on the inputs it receives. GenAI often involves the use of machine learning models to create outputs that are novel and not explicitly programmed.

Hallucination (in AI context): Refers to instances where AI systems generate false or misleading information. This can occur due to limitations in the AI's understanding or the data it has been trained on.

Intellectual Property: Legal rights that arise from intellectual activity in the industrial, scientific, literary, and artistic fields. These rights allow creators to protect and benefit from their creations.

Large Language Models (LLMs): These are advanced AI models trained on vast datasets to process and generate human-like outputs. LLMs can understand and respond to queries, create content, and even engage in conversation.

Misinformation: The spread of false or inaccurate information, often without malicious intent. Misinformation can be due to errors, misunderstandings, or lack of information.

Plagiarism: The act of using someone else's work, ideas, or expressions without proper acknowledgment or permission, presenting them as one's own. Plagiarism is considered unethical and can violate copyright laws.

Predictive AI: AI systems that analyze data to predict future events or outcomes. These systems use historical data and statistical algorithms to forecast what might happen under different scenarios.

Reactive AI: A type of AI that responds to inputs and stimuli without retaining or learning from past interactions. It is limited to immediate responses and does not have memory or learning capabilities.