DIGITAL EDUCATION COUNCIL

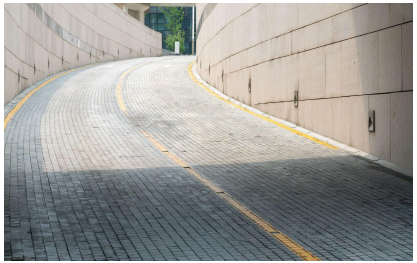
DEC Executive Briefing #015 | March 2025

A Global Map of Policy and Regulation for AI in Higher Education

Key Takeaways

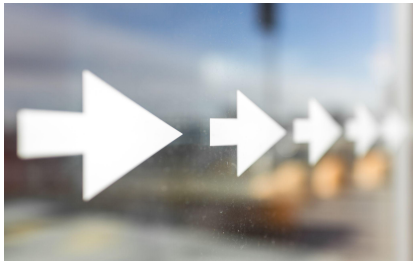
Three regulatory mechanisms

Regulation of AI use and development can often be classified into three regulatory mechanisms: voluntary principles, mandatory standards, and laws and regulations. These mechanisms may function as different stages of a policy process, or may stand alone as a jurisdiction's sole regulatory mechanism.



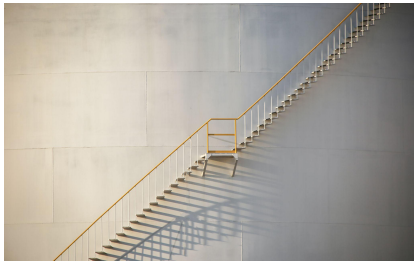
Three regulatory approaches

AI regulations and policies often take one of three approaches: risk-based, principle-based, and use case-based. A risk-based approach regulates AI systems based on potential risks. A principle-based approach provides baseline principles for regulation. A use case-based approach has multiple sets of regulations, each for a specific use case.



12 principles for higher education AI regulation

Twelve principles cover common concerns and principles addressed in regulations, with ethics and human-centricity at the core. This allows for human critical thinking and ethical judgement to remain central in AI applications in higher education. Other key principles include literacy, transparency and explainability, as well as accountability and governance.



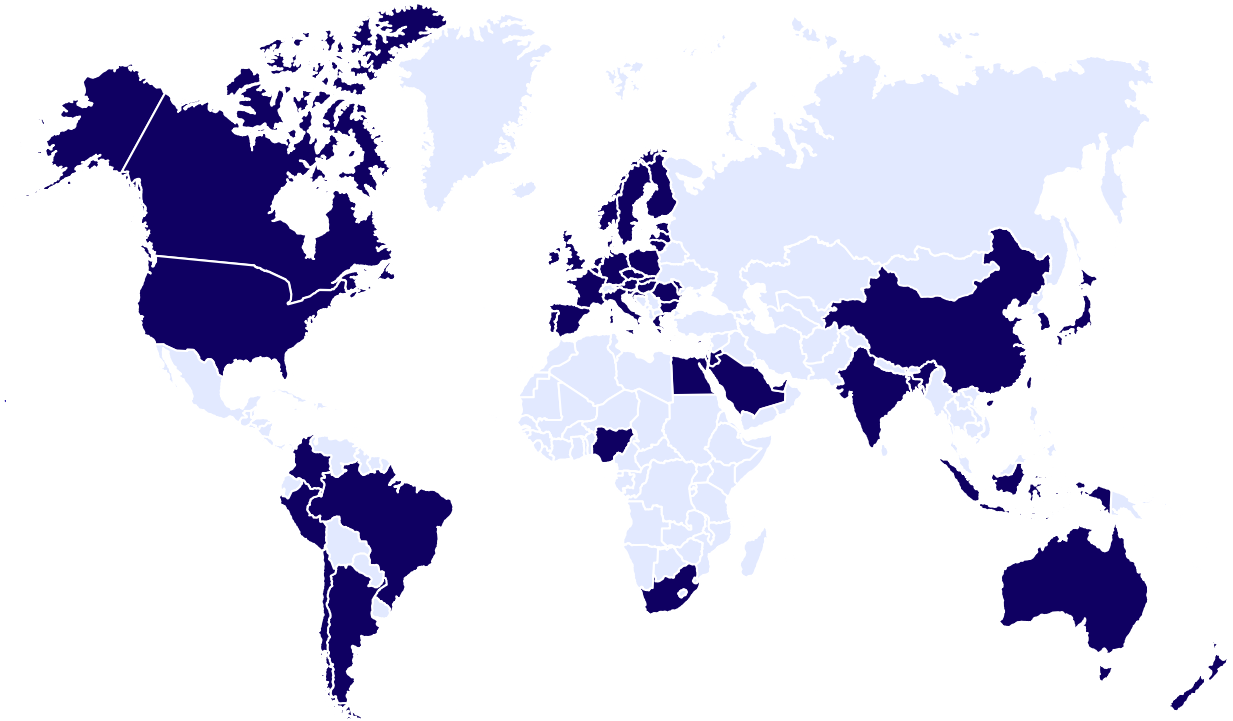
6 DEC AI Regulation Reference Cards

DEC has published six reference cards for institutions to utilise in navigating compliance with AI regulations and guide AI implementation in higher education, according to six common areas of regulation: ethics and human-centricity, AI adoption and implementation, AI use, governance and monitoring, communication, and sustainable growth.

Table of Contents

1. Global AI Policy Mapping

Global Map: Focus Jurisdictions



Asia	Bangladesh China India Indonesia Japan Singapore South Korea
EMEA	Egypt European Union Israel Jordan Saudi Arabia United Arab Emirates United Kingdom
North America	United States of America Canada
Oceania	Australia New Zealand
LATAM	Argentina Brazil Chile Colombia Peru
Africa	Mauritius Nigeria South Africa

AI-Specific Policy Mapping

Voluntary → Regulatory

	Voluntary principles, guidelines, standards	Mandatory principles, guidelines, standards	Law and regulations
Asia	Model AI Governance Framework (SG) AI Guidelines for Business Ver 1.0 (JP) AI National Strategy (ID)	National AI Policy (BD) Principles for Responsible AI (IN)	AI Basic Act (KR) Interim Measures for the Management of Generative Artificial Intelligence Services (CN) Provisions on the Administration of Deep Synthesis of Internet-based Information Services (CN)
EMEA	National Strategy for AI (AE) Pro-innovation Regulatory Framework (UK) AI Strategy (JO) National AI Strategy (EG) AI Ethics Principles (SA) AI Regulations and Ethics (IL)		EU AI Act
North America	NIST Voluntary AI Risk Management Framework (US) Blueprint for an AI Bill of Rights (US)	Executive Order 13859: Maintaining American Leadership in Artificial Intelligence (US)	Artificial Intelligence and Data Act (CA)* Illinois Supreme Court Policy on AI (State-level) Colorado AI Act (State-level)

This is a non-exhaustive map of AI-specific policy.
*Policy is still in proposal/draft stage

AI-Specific Policy Mapping

Voluntary → Regulatory

	Voluntary principles, guidelines, standards	Mandatory principles, guidelines, standards	Law and regulations
Oceania	Voluntary AI Safety Standards (AU) Trustworthy AI in Aotearoa (NZ) Approach to Work on Artificial Intelligence (NZ)		Policy for the Responsible Use of AI in Government (AU) Proposals Paper for Introducing Mandatory Guardrails for AI in High-risk Settings (AU)*
LATAM	Draft National AI Plan (AR)	National Artificial Intelligence Policy Document CONPES 4144 (CO)	Proposed AI National Policy (CL)* AI Bill (BR) Draft Regulation of Law No. 31814 (PE)*
Africa	National AI Strategy (NG) AI Policy Framework (ZA)	AI Policy (MU)	
Others	AI Principles (OECD) UNESCO Recommendations on the Ethics of AI (UN)		

This is a non-exhaustive map of AI-specific policy.
*Policy is still in proposal/draft stage

Balancing Voluntary, Mandatory, and Regulatory Mechanisms

Mixed Approach

Jurisdictions may adopt a combination of approaches to regulate AI innovation. They may apply voluntary mechanisms, such as guidelines or principles, to guide AI development in general, alongside mandatory and enforceable regulatory mechanisms to govern AI use for high-risk AI systems in various industries.

Example: Australia

Australia utilises two instrument types to guide and regulate its AI development and use.

Voluntary mechanism

- Voluntary AI Safety Standards

Regulatory mechanism

- Proposals paper for introducing mandatory guardrails for AI in high-risk settings
- Policy for the responsible use of AI in government

Voluntary Framework as a Regulatory Step or Choice

Jurisdictions may utilise voluntary frameworks as precursors to binding regulations, acting as a placeholder while legislation follows due process.
Other jurisdictions intentionally adopt voluntary mechanisms so as to follow a pro-innovation, light-touch approach in their regulatory framework.

Example: Egypt

Egypt published voluntary guidelines, the *Egyptian Charter for Responsible AI*, to raise awareness of AI ethics as part of their larger National AI Strategy. AI regulation in Egypt is in its final stage of development.

Example: United Kingdom

The UK sets out a pro-innovation regulatory framework, outlining five key non-statutory principles. Individual sectors are expected to incorporate these principles to their industry.

Broader, Related Regulations

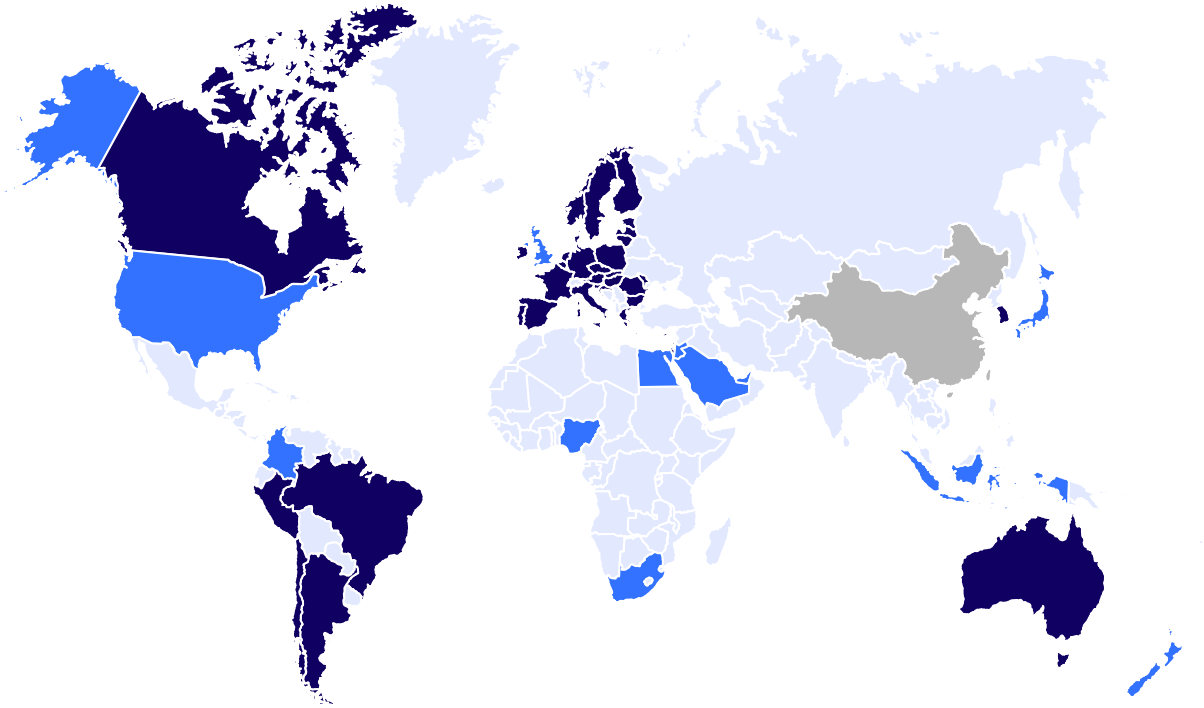
AI development and deployment are also governed by broader, non-AI-specific regulations, such as those on data privacy, employment, competition, and intellectual property. Some jurisdictions have also updated existing regulations to address AI governance.

Relevant Regulations for AI include:

- Data privacy
- Intellectual property
- Employment
- Competition
- Industry-specific regulation

This is a non-exhaustive map of AI-specific policy.

Mapping Global AI Policy Approaches



Three key approaches are emerging to guide and regulate AI development and use.

Risk-Based Approach

A risk-based approach in AI regulation categorises AI systems based on their potential risks and ensures that obligations are proportionate to the risk level.

Principle-Based Approach

The principle-based approach involves creating a set of baseline principles upon which AI use should be regulated, by legislation or voluntary frameworks.

Use Case-Based Approach

The use case-based approach involves publishing multiple regulatory documents, each focusing on regulating a specific use case or technology.

This is a non-exhaustive map.
*Federal-level policies in the US are principle-based. However, state-level policies may differ in approaches.

Global AI Policy Mapping: Risk-Based Approaches

AI regulation approach
Risk-Based

A risk-based approach in AI regulation categorises AI systems based on their potential risks and ensures that obligations are proportionate to the risk level.

Key Features

> **Risk classification**

> **Requirements and obligations**

Risk-based AI regulation varies across jurisdictions, with differences observed in risk classification frameworks and the requirement imposed on AI systems, AI providers, and AI deployers.

Key jurisdiction	Regulation	Risk classification	Requirements and obligations
EU	EU AI Act	• Prohibited AI practices • High-risk • Limited-risks	• Specific obligations for high-risk AI providers, deployers, and other parties • Transparency obligations for limited-risk AI
Brazil	AI Bill	• Excessive-risk • High-risk	• Prohibits excessive-risk AI systems • Specific obligations set for high-risk AI systems
Canada	Artificial Intelligence and Data Act (AIDA)	• Only high-risk AI systems • No prohibited AI systems	• Guided by six principles. Obligations for high-risk AI systems have not been specified.
South Korea	AI Basic Law	• Only high-risk AI systems • No prohibited AI systems	• Specific obligations set for high-impact AI system providers
Australia	Proposals Paper for Introducing Mandatory Guardrails for AI in High-risk Settings	• Only high-risk AI systems • No prohibited AI systems	• Proposed 10 mandatory guardrails for high-risk AI systems

This is a non-exhaustive list of AI regulation.

Risk Assessment and Classification Approaches Vary

> **Risk classification**

Four key risk assessment and classification approaches have been observed in current regulation practices

List-Based

Regulations explicitly list AI systems categorised by risk levels.

EU AI Act defines eight types of AI systems as "unacceptable risk" and outlines high-risk AI applications across eight sectors, including education.

Brazil's *AI Bill* defines 4 types of excessive and 6 types of high-risk AI systems such as AI in the health sector.

High-risk AI system list defined

Factor-Based

AI risk levels are determined by assessing multiple factors, such as the severity of potential harm and scale of use.

Canada's *AIDA* considers 7 key risk determination factors to assess AI system risk levels, such as the difficulty to opt-out from the AI system and the degree to which the AI risks are adequately regulated under another law.

High-risk AI system examples provided

Criteria-Based

AI risk classification is guided by a set of criteria. For example, whether sensitive information is used in the AI system's training.

Australia's *Voluntary AI Safety Standard* includes a risk-assessment toolkit that outlines five key system attributes and a set of guiding questions to help organisations assess the risk level of their AI systems.

High-risk AI system examples provided

Definition-Based

High-risk AI systems are defined by definitions and principles.

South Korea's *AI Basic Law* considers AI systems that pose significant risks or impacts on human life, physical safety, or fundamental rights as high-impact systems.

Australia's *Proposals Paper for Introducing Mandatory Guardrails for AI in High-risk Settings* proposes 6 principles to define high-risk AI systems.

No high-risk AI system examples provided

This is a non-exhaustive list of AI regulation.

Requirements and Obligations for High-Risk AI Systems

DIGITAL EDUCATION COUNCIL

> Requirements and obligations

Regulations across jurisdictions impose varying obligations on high-risk AI systems.

- **The EU AI Act** outlines specific requirements for stakeholders, including AI providers and deployers.
- **Canada's AIDA** provides guiding principles, such as Human oversight & Monitoring, for high-risk AI systems rather than specific obligations.
- **Australia** has proposed 10 guardrails to guide the governance of high-risk AI systems.

Key requirements and obligations fall into six categories:

Assessment
- Conduct conformity assessment
- Conduct impact assessment

Governance
- Publish accountability structures
- Designate accountable actors
- Take the necessary corrective actions

Safety & Security Measures
- Implement risk management processes
- Implement quality management systems
- Implement data governance measures

Human Oversight & Monitoring
- Ensure human oversight
- Monitor AI performance continuously

Transparency & Contestability
- Inform users of AI content and decisions
- Establish contestability mechanism

Record-Keeping
- Keep documentation
- Keep logs automatically generated by high-risk AI systems

Global AI Policy Mapping: Principle-Based Approaches & Sectoral

AI regulation approach
Principle-Based

The principle-based approach involves creating a set of baseline principles upon which AI use should be regulated, by legislation or voluntary frameworks.

Key Features

> **Encourage sectoral regulation**

> **No specific obligations**

Principle-based approach has various rationales: guiding responsible AI development or promoting sector-based guidelines. Regulators often provide supplementary guidance to support implementation.

Jurisdiction	Guidelines	Notable Principles	Key Rationale
UK	A pro-innovation approach to AI regulation Policy Paper	**5 guiding principles** such as: Fairness, Contestability and Redress.	Promote sector-based approach
Singapore	Model AI Governance Framework for Generative AI	**9 focused dimensions** such as: Accountability, Data, Testing and Assurance	Guide responsible development
Japan	AI Guidelines for Business Ver 1.0	**10 principles** such as: Human-Centric, Innovation, Education/Literacy	Guide responsible development
OECD	AI principles	**5 principles**, such as: Inclusive growth, Sustainable Development and Well-being	Guide policy makers worldwide

Guidance for Regulators

UK has published Initial Guidance for Regulators to implement the UK's AI regulatory principles. This guidance include key considerations, questions, and technical standards for sector regulators to refer to.

Support for AI Developers

Singapore developed AI Verify, an AI governance testing framework and software toolkit that tests AI systems performance against a set of 11 AI ethics principles.

This is a non-exhaustive list of AI regulation.

Global AI Policy Mapping: Use Case-Based Approaches

AI regulation approach
Use Case-Based

The use case-based approach involves publishing multiple regulatory documents, each focussing on regulating a specific use case or technology.

Key Feature

> **Application-specific rules**

China

As a key jurisdiction adopting this approach, **China** has issued **three key regulations** relating to AI development and deployment governance, each focussing on specific AI applications with tailored requirements and obligations. These regulations apply to all AI providers operating within the covered applications (with exceptions), regardless of their risk level.

Regulation	Scope	Key requirements and obligations
Generative AI Regulation	Applies to generative AI services that produce text, images, audio, and videos.	• Ensure training data quality, accuracy, objectivity, and diversity • Label content produced by Gen AI • Respect intellectual property
Deep Synthesis Regulation	Applies to the provision of internet information services using deep synthesis technology	• Prohibits the creation, publication, or dissemination of false information • Requires user ID verification • Label deeply synthesised content
Algorithmic Recommendation Regulation	Applies to the use of algorithmic recommendation technology to provide internet information services	• Ensure human intervention and promote positive content • Algorithms must not induce addiction, excessive consumption, or unethical behavior • Provide opt-out option

This is a non-exhaustive list of AI regulation.

A Mixed Approach: US Case Study

Federal Level

Mandatory guidelines and standards for the federal government.

Executive Orders
Executive Order 13859 "Maintaining American Leadership in Artificial Intelligence" and Executive Order 13960 "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government" provide a pro-innovation direction for the use and development of AI, with the aim of fostering public trust and confidence in the use of AI.

Voluntary, non-binding frameworks and guidelines for public and private sectors.

Frameworks
Documents such as the National Institute of Standards and Technology AI Risk Management Framework and the Guidance for Regulation of AI Applications detail non-binding guidelines that centre around building public trust in AI, managing the risks associated with AI use, as well as ensuring ethical, human-centric AI use, along with privacy and non-discrimination.

State Level

State-level legislation and regulation consists of **a mixed approach**: the risk-based approach, the principle-based approach, and the use case-based approach. Each state has their independent legislation for regulating AI use and development.

Risk-Based Approach

Example:
Massachusetts HD4053

HD4053 is proposed legislation aimed at protecting consumers from discrimination by high-risk AI systems. The bill defines high-risk AI systems as AI operated without human oversight to make decisions about key areas such as housing, education and healthcare. The bill mandates that AI developers use reasonable care to protect consumers against algorithmic discrimination by a high-risk AI system.

Principle-Based Approach

Example:
California AI Transparency Act

This act mandates businesses providing a generative AI system with over 1 million monthly users to provide detection tools allowing users to find out more about how AI was used within their content or products. It also requires businesses to disclose the use of AI-generated content. This act operates on a commonly-seen principle of transparency on AI use, where AI use is disclosed and available for further inspection.

Use Case-Based Approach

Example:
Illinois AI Video Interview Act

This act applies to employers utilising AI to conduct video interviews during hiring. It requires employers to notify applicants of AI use, and explain how AI will be used in the process, as well as how AI will evaluate applicants, before obtaining an applicant's' consent. This act serves to regulate a specific use case of AI as an interviewing and recruitment tool.

This is a non-exhaustive list of AI regulation.

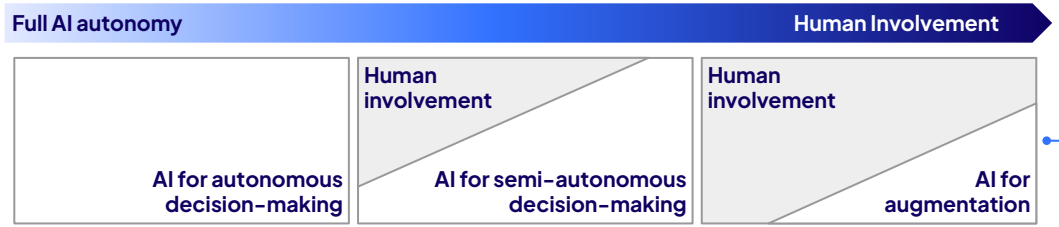
2. Global AI Policy Impact on Higher Education

High-Risk AI Systems to Watch Out for in Higher Education

Based on risk-based regulations that classify AI systems as **unacceptable/excessive risk or high risk**, several AI applications in higher education are already regulated or likely to face regulation. These systems can be broadly categorised into three groups: **AI-driven access to resources, AI for security and surveillance, and AI for integrity monitoring.**

Access to Opportunity	AI in admission decisions	AI to assess appropriate level of education for students	AI for scholarships and funding allocation	AI to evaluate learning outcomes		AI systems that decide the access to critical resources and opportunity, make the final decision, or replace critical human role
Security & Surveillance	AI-driven campus security system	AI categorising students based on biometric data	AI tracking students using biometric recognition	Emotion recognition in class, exams, and counselling	Student facial data scraping without permission	AI systems that serve as safety components, or scrape, track, and use biometrics data
Integrity Monitoring	AI monitoring and detecting dishonesty during tests	Student dishonesty prediction	AI-based student reputation scoring			AI systems that monitor, detect, and predict individual's integrity

AI Innovation in Education Moving Toward Greater Human Oversight



Example human involvement shift

Admission	Prohibited: AI makes final admission decision	AI ranks or filters applicants based on predefined criteria	AI provides insights about applicants instead of filtering
Teaching & Learning	AI predicts and automatically intervenes with at-risk students	AI alerts instructors of at-risk students	
Assessment		AI grades subjective assignments	AI provides feedback for grading considerations
Administration		AI evaluates financial aid eligibility	AI suggests funding options to inform human judgement

Innovation shift

Human Involvement vs AI Autonomy

The risk-based approach views the **lack of human oversight** as a **high-risk factor**, with fully autonomous AI decision-making subject to strict regulation or prohibition.

According to the DEC AI Governance Framework, institutions should be cautious with a human-out-of-the-loop approach and prioritise AI innovations that keep humans in the loop.

For the three human involvement approaches, Digital Education Council Members please refer to:

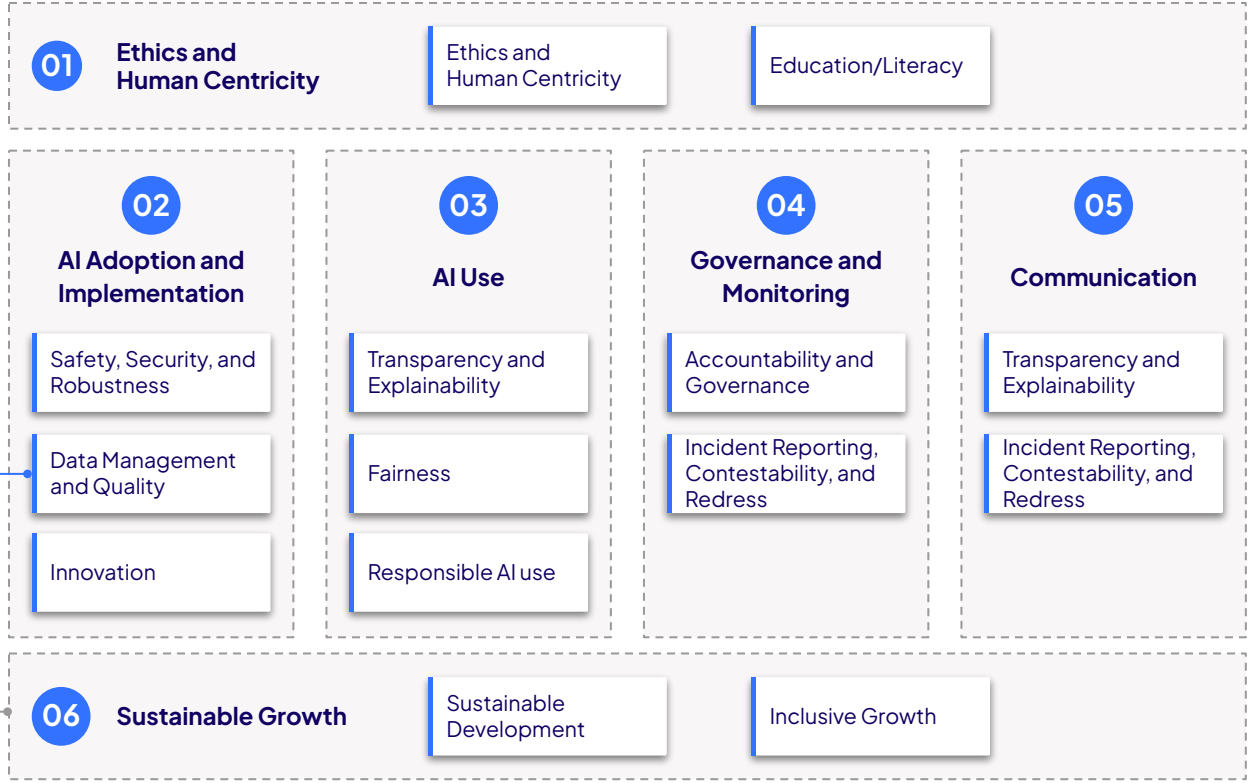
- DEC Executive Briefing #006 - Solving the AI Governance Problem

Principle-Based AI Compliance Framework for Higher Education

Institutions can achieve compliance by following twelve key principles across six areas, with Ethics and Human Centricity as the guiding pillar.

12
Key Principles

6
Compliance Areas



AI Compliance Reference Card: Ethics & Human Centricity

01

Ethics & Human Centricity

AI systems should be developed and deployed in a manner that aligns with human values, ensuring it serves as a tool for human empowerment rather than replacement.

Key Principles

Ethics and Human Centricity

Education/Literacy

Key to Compliance

- Ensure human oversight in AI processes
- Conduct ethical reviews and impact assessment
- Promote inclusivity and diversity
- Train staff & faculty on responsible AI use

Key roles and responsibilities

Leadership

- ☐ What does ethical AI use look like and how do we define it?
- ☐ Do we have a proactive review process for AI adoption?
- ☐ Are there clear guidelines on human oversight for AI-driven decisions?
- ☐ Do we provide adequate AI literacy training?

Faculty

- ☐ Am I using AI in a way that enhances, rather than replaces human judgment?
- ☐ Have I considered the long-term ethical implications of AI tools in my work?
- ☐ Am I actively promoting AI ethics awareness among students?

Staff

- ☐ What are the key ethical concerns that need to be addressed?
- ☐ Have we implemented regular audits of AI systems for ethical concerns?
- ☐ Do we have clear reporting mechanisms for ethical AI concerns?

Red flags to watch for

- AI makes high-stakes decisions without human oversight
- Use AI when the impact on student learning is not clear

Quick wins for compliance

- Add an "AI Ethics" statement for all AI tools used within the institution
- Create an AI & Ethics faculty discussion group

AI Compliance Reference Card: AI Adoption and Implementation

02

AI Adoption and Implementation

Integration of AI must be executed in a manner that ensures safety, security, and robust data management principles.

Key Principles

- **Safety, Security, and Robustness**
- **Data Management and Quality**
- **Innovation**

Key to Compliance

- Assess risks before deployment
- Ensure data quality compliance with data regulations
- Regularly test AI accuracy and reliability

Key roles and responsibilities

Leadership

- ☐ Do we have an AI risk & security policy in place?
- ☐ Is there a dedicated team or role responsible for overseeing AI compliance and security?
- ☐ What information is needed to demonstrate security?
- ☐ Is there a process to identify beneficial AI use cases?

Faculty

- ☐ Have I assessed the potential risks of AI tools used in my work?
- ☐ Am I actively identifying beneficial AI use cases?
- ☐ Am I aware of the data quality and data source of AI tools?
- ☐ Have I checked if the AI tools I use comply with institutional policies and local regulations?

Staff

- ☐ Have we implemented regular security audits for AI tools?
- ☐ Do we require transparency documents from AI providers, such as details on AI functionality?
- ☐ Are we aware of proper data management processes when working with AI?

Red flags to watch for

- No dedicated policy for AI security and data management
- No dedicated AI safety oversight team
- AI models trained on biased or outdated data

Quick wins for compliance

- Limit sensitive data AI systems can access
- Ask AI providers for security and compliance documents before purchasing
- Host an AI security briefing for faculty & staff

AI Compliance Reference Card: AI Use

03

AI Use

Use of AI and its processes should be transparent, with an emphasis on explainability and fairness throughout.

Key Principles

- **Transparency and Explainability**
- **Fairness**
- **Responsible AI use**

Key to Compliance

- Define appropriate AI use
- Operate in accordance with instructions of use
- Explain AI decision-making
- Implement safeguards to prevent biases

Key roles and responsibilities

Leadership

- ☐ Do we have policies requiring documents explaining AI systems and their use?
- ☐ Do we have guidelines to define appropriate AI use?
- ☐ Do we have processes to audit AI systems for bias and fairness?

Faculty

- ☐ Can I clearly explain how AI tools I use make decisions?
- ☐ Do I actively monitor AI-generated output to detect potential biases or unfair patterns?
- ☐ Have I clearly defined appropriate use of AI in course policies?

Staff

- ☐ Have we implemented regular fairness and bias audits for AI tools used within the institution?
- ☐ Is there sufficient human oversight in AI-driven decisions, especially for high-impact areas like admission?
- ☐ Is AI use in administrative processes clearly disclosed?

Red flags to watch for

- AI decisions are not understandable by users
- AI recommendations disproportionately affect certain groups

Quick wins for compliance

- Include AI function explanation statement in AI use
- Ensure AI systems have opt-out options for students
- Run AI fairness training for faculty & staff

AI Compliance Reference Card: Governance and Monitoring

04

Governance and Monitoring

Clear accountability structures must govern AI, ensuring responsible oversight and channels for reporting and challenging AI decisions.

Key Principles

Accountability and Governance

Incident Reporting, Contestability, and Redress

Key to Compliance

- Assign clear roles and responsibilities for AI oversight
- Ensure compliance with AI regulations
- Keep records and logs
- Create incident response protocols

Key roles and responsibilities

Leadership

- ☐ Who are the key stakeholders that should be involved in the governance process?
- ☐ What are the responsibilities of each stakeholder?
- ☐ Have we established a process for reviewing and updating AI policies?

Faculty

- ☐ What is my responsibility regarding the use of AI?
- ☐ Do I know who to contact for AI governance concerns?
- ☐ Am I aware of the corrective actions I need to take if an AI tool is flagged for non-compliance?

Staff

- ☐ Do we maintain an inventory of all AI systems used on campus?
- ☐ Are our AI compliance policies effectively enforced, with regular assessments and updates?
- ☐ What are the reporting mechanisms in place for any incidents of misuse of AI?

Red flags to watch for

- No official oversight body for AI
- No or out-of-date AI policies
- AI systems are adopted without review

Quick wins for compliance

- Develop and publish an institution-wide AI governance policy
- Require AI tools to have a human accountability layer

AI Compliance Reference Card: Communication

05

Communication

AI use and processes should be transparent, with clear channels for reporting issues, challenging outcomes, and ensuring fairness.

Key Principles

Transparency and Explainability

Incident Reporting, Contestability, and Redress

Key to Compliance

- Publish comprehensive and clear AI policies
- Disclose AI use properly
- Establish mechanisms for feedback and challenging AI decisions
- Use plain language

Key roles and responsibilities

Leadership

- ☐ Are AI-driven processes clearly disclosed in an accessible and understandable manner?
- ☐ Have we created mechanisms for students and staff to challenge AI-driven decisions?
- ☐ How can we support faculty and staff to communicate their AI use?

Faculty

- ☐ Have I disclosed the use of AI in my work?
- ☐ Have I informed students about how to appeal AI decisions?
- ☐ Have I informed students about the appropriate use of AI?
- ☐ Do I know who to contact in case of AI-related concerns or incidents?

Staff

- ☐ Have we set up an AI support/help desk where students, faculty, and staff can ask questions or report issues?
- ☐ What is our protocol for responding to AI incidents?
- ☐ Do we have a feedback loop to improve AI systems and policies?

Red flags to watch for

- No process for challenging AI decisions
- Faculty and students are unaware of the institution's AI policy or the AI systems used in any processes

Quick wins for compliance

- Mandate AI disclaimers in course syllabi
- Create an AI help centre for faculty & staff

AI Compliance Reference Card: Sustainable Growth

06

Sustainable Growth

AI should contribute to environmental, social, and economic sustainability, ensuring responsible use and equitable access and achieving inclusive growth.

Key Principles

Sustainable Development

Inclusive Growth

Key to Compliance

- Understand the sustainability implications of AI
- Ensure sustainability is a key consideration in AI adoption and use
- Ensure equitable AI access

Key roles and responsibilities

Leadership

- ☐ Have we assessed the environmental, social, and economic implications of AI adoption within our institution?
- ☐ Do we have a strategy to balance AI adoption with sustainability efforts, such as reducing energy consumption or promoting ethical AI use?

Faculty

- ☐ Have I assessed the environmental and social impact of the AI tools I use in my work?
- ☐ Do I educate students on AI's impact on sustainability and responsible AI practices?
- ☐ How do I use AI to help increase inclusiveness in my classes?

Staff

- ☐ Do we have a responsible procurement process for AI tools?
- ☐ Are we tracking and reducing AI's environmental footprint within our institution?
- ☐ Are AI vendors evaluated for sustainability practices before procurement?

Red flags to watch for

- AI systems' environmental impact is not assessed
- AI adoption widens the digital divide
- Sustainability is not considered in AI procurement decisions

Quick wins for compliance

- Prioritise AI tools with low energy consumption
- Introduce a "Sustainable AI" module in courses
- Utilise AI tools in improve accessibility of education to differently abled individuals

Alessandro Di Lullo
Chief Executive Officer
alessandro@digitaleducationcouncil.com

Danny Bielik
President
danny@digitaleducationcoucil.com

Hui Rong
Research and Intelligence Lead
hui@digitaleducationcouncil.com

Charlene Chun
Research and Intelligence Associate
charlene@digitaleducationcouncil.com