



UNIVERSITY GRANTS COMMISSION
SRI LANKA



National Policy Framework for the Use of Artificial Intelligence in the State University System of Sri Lanka

Table of Contents

1. INTRODUCTION	1
1.1. BACKGROUND	1
1.2. NEED FOR A NATIONAL POLICY FRAMEWORK	1
1.3. PURPOSE AND CONTEXT	2
1.4. RATIONALE	2
2. POLICY PRINCIPLES	3
2.1. ENABLEMENT-FIRST APPROACH TO AI ADOPTION	3
2.2. HUMAN-CENTRED AND AI-ASSISTED	3
2.3. FAIR, INCLUSIVE, AND RIGHTS-BASED	3
2.4. TRANSPARENT AND PROPORTIONATE GOVERNANCE	3
2.5. ACADEMIC FREEDOM AND INSTITUTIONAL AUTONOMY	3
2.6. DATA STEWARDSHIP AND SECURE DIGITAL ECOSYSTEMS	3
2.7. CAPACITY BUILDING AND INSTITUTIONAL READINESS	4
2.8. NATIONAL RELEVANCE AND RESPONSIBLE INNOVATION	4
2.9. ENVIRONMENTAL SUSTAINABILITY AND LONG-TERM VIABILITY	4
3. POLICY STATEMENTS	5
3.1. UNIVERSITIES SHALL ADOPT AI IN A MANNER THAT ENHANCES EDUCATION, RESEARCH, AND ADMINISTRATION WHILE SAFEGUARDING ETHICAL STANDARDS.	5
3.2. AI SHALL NOT BE USED AS THE SOLE BASIS FOR HIGH-STAKES DECISIONS AFFECTING STUDENTS OR STAFF.	5
3.3. INDIVIDUALS AFFECTED BY AI-SUPPORTED DECISIONS SHALL HAVE THE RIGHT TO EXPLANATION, REVIEW, AND REDRESS.	5
3.4. AI SYSTEMS SHALL BE SUBJECT TO APPROPRIATE OVERSIGHT, DOCUMENTATION, AND AUDITABILITY.	6
3.5. DATA USED IN AI SYSTEMS SHALL BE MANAGED AS A PUBLIC TRUST, ENSURING PRIVACY, SECURITY, AND INTEROPERABILITY.	6
3.6. INSTITUTIONS SHALL ENSURE EQUITABLE ACCESS TO INSTITUTIONALLY ADOPTED AI-ENABLED SYSTEMS AND SERVICES, INCLUDING REASONABLE ACCOMMODATIONS FOR PERSONS WITH DISABILITIES.	6
3.7. UNIVERSITIES SHALL INVEST IN INFRASTRUCTURE, GOVERNANCE, AND HUMAN CAPACITY TO SUPPORT AI ADOPTION.	6
4. POLICY GOALS	7
4.1. UNIVERSAL INSTITUTIONAL POLICY ADOPTION	7
4.2. GOVERNANCE STRUCTURES ESTABLISHED ACROSS THE SECTOR	7
4.3. BASELINE AI LITERACY ACROSS THE UNIVERSITY COMMUNITY	7
4.4. EQUITABLE AND ACCESSIBLE AI INTEGRATION	7
4.5. RISK GOVERNANCE OPERATIONAL FOR HIGH-RISK AI SYSTEMS AND HIGH-STAKES DECISIONS.	7
4.6. CONTRIBUTION TO NATIONAL AI DEVELOPMENT	7

5. APPLICABILITY AND SCOPE	8
5.1. INSTITUTIONALLY ADOPTED AI SYSTEMS.....	8
5.2. INDIVIDUAL USE OF EXTERNALLY AVAILABLE AI TOOLS.....	8
5.3. THE BOUNDARY IN PRACTICE	8
6. POLICY IMPLEMENTATION.....	10
6.1. FOUNDATIONAL DIGITAL INFRASTRUCTURE	10
6.1.1. MINIMUM INFRASTRUCTURE READINESS.....	10
6.1.2. CONNECTIVITY, SECURITY, AND RESILIENCE	10
6.1.3. COMPUTING AND DATA SYSTEMS.....	11
6.1.4. PLATFORMS, INTEROPERABILITY, AND ACCESSIBILITY	11
6.1.5. SHARED INFRASTRUCTURE, COMMON STANDARDS, AND INSTITUTIONAL DIFFERENTIATION.....	11
6.1.6. REVIEW AND CONTINUOUS IMPROVEMENT.....	12
6.2. RISK-BASED AI GOVERNANCE	12
6.2.1. RISK LEVELS	12
6.2.2. LIFECYCLE GOVERNANCE	14
6.2.3. MANDATORY RISK CONSIDERATIONS	14
6.3. GOVERNANCE, ACCOUNTABILITY AND SAFEGUARDS.....	15
6.3.1. INSTITUTIONAL ACCOUNTABILITY FOR AI SYSTEMS	15
6.3.2. GOVERNANCE STRUCTURES AND INTERNAL OVERSIGHT.....	15
6.3.3. MONITORING, AUDIT, AND COMPLIANCE MECHANISMS	15
6.3.4. LEGAL AND ETHICAL COMPLIANCE	16
6.3.5. RESOURCING FOR GOVERNANCE AND SAFEGUARDS	16
6.3.6. INCLUSIVE GOVERNANCE AND ACCESSIBILITY OVERSIGHT.....	16
6.4. INSTITUTIONAL DECISION-MAKING AND SERVICES.....	16
6.4.1. HUMAN OVERSIGHT IN HIGH-STAKES DECISIONS.....	16
6.4.2. TRANSPARENCY OF AI USE.....	16
6.4.3. RIGHT TO EXPLANATION AND APPEAL	16
6.4.4. FAIRNESS AND NON-DISCRIMINATION.....	17
6.4.5. DOCUMENTATION AND AUDITABILITY	17
6.4.6. ACCESSIBILITY AND REASONABLE ACCOMMODATION	17
6.5. ACADEMIC PRACTICE, INTEGRITY AND COMMUNICATION	17
6.5.1. SYSTEM-WIDE AI VOCABULARY AND GLOSSARY	17
6.5.2. SHARED STANDARDS FOR AI USE AND INTEGRITY	17
6.5.3. MINIMUM STANDARDS FOR TRANSPARENCY AND FAIRNESS	17
6.5.4. SYSTEM COORDINATION AND CONSISTENCY	17
6.5.5. INTEGRATION INTO QUALITY ASSURANCE	18
6.5.6. GOOD PRACTICE AND KNOWLEDGE SHARING	18
6.5.7. ACADEMIC INTEGRITY AND RESPONSIBILITY	18
6.5.8. HUMAN OVERSIGHT IN HIGH-STAKES ACADEMIC DECISIONS.....	18
6.5.9. TRANSPARENCY OF AI USE.....	18
6.5.10. REDRESS AND APPEAL MECHANISMS	18
6.5.11. ADOPTION AND CONTEXTUAL EXTENSION OF STANDARDS	18
6.5.12. CURRICULUM AND PEDAGOGICAL ADAPTATION.....	19
6.5.13. ALIGNMENT AND COMPLIANCE WITH UGC STANDARDS.....	19
6.6. CAPACITY, LITERACY AND IMPLEMENTATION	19
6.6.1. AI LITERACY STANDARDS (BASELINE DEFINITION & MAINTENANCE)	19

6.6.2. SYSTEM-WIDE IMPLEMENTATION AND MONITORING.....	19
6.6.3. KNOWLEDGE SHARING AND CAPACITY BUILDING ECOSYSTEM	19
6.6.4. RECOGNITION AND INCENTIVES FOR GOOD PRACTICE	19
6.6.5. AI LITERACY IMPLEMENTATION AND TRAINING	19
6.6.6. CONTINUOUS UPDATING OF AI CAPACITY	19
6.6.7. HUMAN OVERSIGHT AND INSTITUTIONAL CAPABILITY	20
6.6.8. INCLUSIVE AND ACCESSIBLE AI LEARNING.....	20
6.6.9. REPORTING AND ACCOUNTABILITY TO UGC	20
6.6.10. MULTILINGUAL AND CONTEXTUAL CAPACITY BUILDING	20
6.6.11. INSTITUTIONAL FLEXIBILITY IN DELIVERY	20
6.6.12. ROLE OF STAFF DEVELOPMENT CENTRES.....	20
6.7. DATA, SYSTEMS AND PROCUREMENT	20
6.7.1. DATA GOVERNANCE REVIEW BEFORE AI DEPLOYMENT	20
6.7.2. PROTECTION OF SENSITIVE AND INSTITUTIONAL DATA	21
6.7.3. PROCUREMENT SAFEGUARDS FOR AI SYSTEMS	21
6.7.4. VENDOR AND PARTNER ACCOUNTABILITY	21
6.7.5. LIMITS ON SECONDARY USE OF UNIVERSITY DATA	21
6.7.6. DOCUMENTATION AND SYSTEM REGISTERS	21
6.7.7. LOCAL RELEVANCE AND LANGUAGE CONSIDERATIONS	21
6.7.8. SHARED INFRASTRUCTURE AND POOLED EXPERTISE.....	22
6.7.9. ALIGNMENT WITH LEGAL AND INSTITUTIONAL REQUIREMENTS.....	22
6.8. INNOVATION, PARTNERSHIPS AND FUNDING	22
6.8.1. PROMOTION OF AI RESEARCH AND INNOVATION	22
6.8.2. RESPONSIBLE PARTNERSHIP GOVERNANCE	22
6.8.3. SAFEGUARDS FOR HIGH-IMPACT INNOVATION INITIATIVES.....	23
6.8.4. ASSESSMENT OF RISKS AND BENEFITS IN COLLABORATIONS	23
6.8.5. MULTI-UNIVERSITY COLLABORATION AND SHARED PLATFORMS.....	23
6.8.6. EQUITABLE ACCESS TO FUNDING AND INNOVATION OPPORTUNITIES	23
6.8.7. COMMERCIALISATION, ENTREPRENEURSHIP, AND INTELLECTUAL PROPERTY	23
6.8.8. TRANSPARENCY IN MATERIAL PARTNERSHIP ARRANGEMENTS.....	23
6.8.9. LOCAL LANGUAGE AND CONTEXT-SENSITIVE AI RESOURCES.....	23
6.8.10. ALIGNMENT WITH PUBLIC INTEREST AND NATIONAL PRIORITIES	24
6.9. MONITORING, EVALUATION AND ADAPTATION	24
6.9.1. MONITORING AND EVALUATION	24
6.9.2. QUALITY ASSURANCE AND SYSTEM-LEVEL OVERSIGHT	25
6.9.3. REVIEW CYCLE	25
6.9.4. CONTINUOUS IMPROVEMENT AND ADAPTIVE UPDATES	25
6.9.5. INTERIM GUIDANCE, CLARIFICATIONS, OR ADVISORIES	26
7. GLOSSARY	27
8. REFERENCES.....	32
9. AI POLICY FRAMEWORK DEVELOPMENT TEAM.....	34

1. Introduction

1.1. Background

Artificial Intelligence (AI) is reshaping higher education systems globally, with universities rapidly integrating AI into teaching, research, and administration. For the purposes of this framework, AI refers to machine-based systems capable of performing tasks that typically require human intelligence, including prediction, classification, recommendation, decision support, and content generation. Sri Lanka's state universities are part of this shift. AI is now deeply embedded in institutional life, shaping how students learn, how faculty teach and conduct research, and how universities manage academic and administrative processes.

This adoption is uneven across the university sector. Students use AI tools to clarify concepts, draft and refine writing, and prepare for assessment. Faculty use AI to develop teaching materials, support research workflows, and identify potential academic misconduct. Administrative units are beginning to explore AI for institutional services. While some institutions and faculties have developed local AI policies, these remain limited and unevenly distributed across the system. In many contexts, AI-related practice is still shaped by individual, departmental, or institutional judgment rather than shared standards or coordinated governance.

The consequences of this gap are increasingly visible. Students face uncertainty about acceptable AI use, including inconsistent expectations and the unreliable application of detection tools. Access to advanced AI systems varies, with some students and staff able to use premium tools while others rely on limited free versions, raising equity concerns within and across institutions. Overreliance on AI in early-stage learning risks undermining the development of foundational skills. Faculty require support to integrate AI effectively into teaching and assessment. Administrative staff increasingly encounter AI-enabled systems in areas such as student services, human resources, and institutional reporting, often without clear guidance on appropriate use, oversight responsibilities, or the limits of automation. Institutional data entered into external systems raises concerns related to privacy, security, and ownership. In high-stakes contexts, including admissions, grading, and disciplinary processes, the absence of clear expectations for oversight, accountability, and transparency introduces risks for individuals and institutions.

1.2. Need for a National Policy Framework

The challenges described above share a common feature: they operate at the level of the system as well as the institution. No single university, however well-resourced, can resolve them alone.

Developing robust governance frameworks, building secure and interoperable infrastructure, ensuring equitable access to AI tools and support, and establishing consistent safeguards for high-stakes decisions all require coordination, shared standards, and resources that individual institutions are structurally limited in providing independently. Without a common framework, universities face pressure to act in isolation — producing duplicated effort, uneven protection for students and staff, and fragmented practice that disadvantages the students and institutions least equipped to navigate the gaps.

A system-level response is therefore not merely preferable — it is necessary. The University Grants Commission is the appropriate body to provide that response, with the authority and reach to establish shared principles, set minimum standards, support institutions with differentiated capacity, and ensure that responsible AI adoption becomes a coherent feature of Sri Lanka's public university sector rather than an uneven outcome of individual institutional decisions. This framework gives that mandate its operational form.

1.3. Purpose and Context

This document establishes a national policy framework for the use of artificial intelligence across Sri Lanka's state university sector. It provides a shared structure to guide how AI is adopted, governed, and integrated across teaching, research, administration, and institutional services.

The framework operates at the system level. It establishes minimum standards that all state universities must meet, and universities retain autonomy in how AI is implemented within their academic, administrative, and research environments. Institutions may extend or strengthen these standards within their local contexts, but shall not fall below them.

This is a framework, not a prescriptive or uniform policy. It does not mandate identical approaches across institutions. Instead, it establishes a common foundation to reduce fragmentation, support responsible adoption, and enable institutions to develop context-appropriate practices within a shared governance structure.

1.4. Rationale

This framework is grounded in the recognition that artificial intelligence presents both significant opportunities and important risks for higher education. Its governance approach is designed to support responsible adoption while maintaining academic integrity, equity, accountability, and public trust.

The framework is situated within Sri Lanka's broader national policy context. *AI Sri Lanka 2028: Sri Lanka's National Strategy on AI* sets out the country's commitment to responsible and inclusive AI development across sectors. The *Personal Data Protection Act, No. 9 of 2022, as amended by the Personal Data Protection (Amendment) Act, No. 22 of 2025*, establishes the legal framework governing the processing and protection of personal data. This framework operationalises those national commitments within the state university sector, translating system-level principles into governance expectations appropriate to the higher education context.

The framework adopts an enablement-first orientation. AI offers genuine potential to improve the quality, reach, and efficiency of teaching, research, and administration across Sri Lanka's universities, and this framework is designed to support that potential. Safeguards are calibrated to the level of risk and potential impact associated with particular systems or contexts of use, ensuring that governance requirements are proportionate rather than uniform. Responsible innovation and appropriate oversight are understood as complementary, not competing, objectives.

The framework also recognises the diversity of Sri Lanka's university sector. Institutions differ in mission, infrastructure, capacity, and readiness. A framework that imposed identical requirements on all institutions regardless of context would create unrealistic burdens for some institutions while under-challenging others. Implementation must therefore be flexible and context-sensitive, allowing institutions to move at a credible pace within a shared system of principles and minimum standards—with the expectation of gradual maturity rather than immediate uniform sophistication.

The following sections set out the principles, policy provisions, and implementation parameters that guide AI adoption and governance across Sri Lanka's state university sector.

2. Policy Principles

2.1. Enablement-First Approach to AI Adoption

AI adoption is guided by an enablement-first approach, with safeguards calibrated to risk. Sri Lanka's universities stand to benefit significantly from AI integration across teaching, research, and administration, and this framework is designed to support that integration rather than impede it. Governance requirements are proportionate to the level of risk and potential impact involved, ensuring that low-stakes uses are not burdened by the same oversight expectations as high-stakes institutional decisions.

2.2. Human-Centred and AI-Assisted

AI use is grounded in human judgment and accountability, with AI functioning in a supportive role. Across Sri Lanka's university sector, decisions that affect students, staff, and institutional life must remain the responsibility of identifiable human authorities. AI systems may inform, assist, and improve those decisions, but they do not replace the judgment, contextual understanding, or accountability that human oversight provides.

2.3. Fair, Inclusive, and Rights-Based

AI use is aligned with equity, accessibility, privacy, and the right to question and review decisions. Sri Lanka's universities serve students and staff across diverse linguistic, socio-economic, and geographic contexts, and AI systems must not reproduce or deepen existing inequities. This principle requires that AI-enabled tools and services are accessible across Sinhala, Tamil, and English language contexts, and that individuals retain meaningful rights to understand and challenge decisions that affect them.

2.4. Transparent and Proportionate Governance

AI governance is risk-based, with transparency and human oversight aligned to context and level of impact. Not all AI use carries the same consequences, and governance expectations should reflect that. Where AI is used in routine, low-stakes functions, basic disclosure is sufficient. Where AI influences decisions with significant consequences for individuals—in admissions, assessment, employment, or disciplinary processes—stronger transparency, documentation, and oversight requirements apply.

2.5. Academic Freedom and Institutional Autonomy

AI adoption respects academic freedom and institutional autonomy within a shared system of principles and minimum standards. This framework establishes a common foundation across Sri Lanka's state universities, but it does not prescribe how individual academics teach, design assessments, or conduct research. Faculty retain the freedom to determine how AI is or is not integrated into their professional practice, and institutions retain the authority to implement the framework in ways that reflect their mission, capacity, and context.

2.6. Data Stewardship and Secure Digital Ecosystems

Data is treated as a public trust, with appropriate safeguards for security, integrity, and responsible use. Sri Lanka's universities hold sensitive data relating to students, staff, and research—data that carries legal, ethical, and institutional obligations. As AI systems increasingly depend on large volumes of data to function, the responsible stewardship of that data becomes inseparable from responsible AI governance. Universities must ensure that data used in AI systems is collected, stored, and processed lawfully, securely, and in the genuine interest of those it concerns.

2.7. Capacity Building and Institutional Readiness

AI literacy and institutional capacity are developed as core, inclusive, and evolving system capabilities. Effective and responsible AI adoption requires more than policy—it requires people who understand what AI systems do, what their limitations are, and how to oversee them appropriately. Across Sri Lanka’s university sector, capacity varies significantly, and this framework recognises that building AI literacy among students, academic staff, administrative staff, and institutional leadership is an ongoing and shared responsibility, not a one-time training exercise.

2.8. National Relevance and Responsible Innovation

AI adoption is aligned with national priorities and supports responsible innovation, public trust, and academic integrity. Sri Lanka’s universities are public institutions with responsibilities that extend beyond their campuses—to contribute to national development, to serve the public interest, and to model responsible practice in a rapidly changing technological landscape. AI-related research, innovation, and partnerships should be pursued in ways that reflect these responsibilities, advancing national priorities while maintaining the ethical standards on which public trust depends.

2.9. Environmental Sustainability and Long-Term Viability

AI adoption is pursued in a manner that is environmentally responsible and sustainable over time. Compute-intensive AI systems carry significant energy and resource costs that are relevant to any institution operating within Sri Lanka’s infrastructure and energy context. Universities should consider the environmental footprint of AI systems they adopt or develop, favour solutions that are energy-efficient and locally sustainable where feasible, and avoid dependencies on platforms or infrastructure that cannot be maintained over the long term. This principle aligns with Sri Lanka’s national sustainability commitments and with the growing international consensus, reflected in UNESCO, OECD, and EU frameworks, that responsible AI governance must account for environmental impact alongside ethical and operational considerations.

3. Policy Statements



3.1. Universities shall adopt AI in a manner that enhances education, research, and administration while safeguarding ethical standards.

AI adoption within universities is intended to improve the quality, efficiency, and reach of core institutional functions, including teaching and learning, research productivity, and administrative services. However, such adoption must be guided by ethical principles, including fairness, accountability, transparency, and respect for human dignity. Universities shall ensure that AI systems are used to augment human capabilities rather than replace them in ways that undermine academic integrity or public trust. All AI-enabled initiatives shall be aligned with institutional values, national priorities, and internationally recognised ethical and governance frameworks.

3.2. AI shall not be used as the sole basis for high-stakes decisions affecting students or staff.

High-stakes decisions—such as admissions, grading, recruitment, promotion, disciplinary action, or termination—have significant consequences for individuals' rights and opportunities. AI systems may be used to support such decisions, but they shall not replace human judgment. A qualified human authority must review and take responsibility for all final decisions, ensuring that contextual factors, fairness considerations, and individual circumstances are appropriately considered. This provision safeguards against automated bias, errors, and lack of accountability.

3.3. Individuals affected by AI-supported decisions shall have the right to explanation, review, and redress.

Any student, staff member, or stakeholder impacted by an AI-supported decision shall be entitled to understand how that decision was made, including the role played by the AI system. Institutions shall provide clear, accessible explanations of AI use, ensure mechanisms for independent review of decisions, and establish fair and timely processes for appeal and redress. These mechanisms must be accessible to all individuals, including persons with disabilities, and shall uphold principles of natural justice and procedural fairness.

3.4. AI systems shall be subject to appropriate oversight, documentation, and auditability.

Institutionally adopted AI systems, and individual or departmental uses involving institutional data, institutional platforms, or consequential decisions within universities shall operate within a framework of institutional oversight. This includes maintaining comprehensive documentation on system purpose, data sources, decision logic (where feasible), risk assessments, and responsible personnel. Systems must be auditable, meaning that their outputs and decision pathways can be reviewed, evaluated, and, where necessary, challenged. Regular monitoring and periodic audits shall be conducted to ensure continued compliance with policy, legal requirements, and performance expectations.

3.5. Data used in AI systems shall be managed as a public trust, ensuring privacy, security, and interoperability.

Data within the university sector, particularly data relating to students, staff, and research, shall be treated as a public trust requiring responsible stewardship, appropriate protections, and accountable governance. Institutions shall ensure that data used in AI systems is collected, stored, processed, and shared in compliance with applicable laws, ethical standards, and institutional policies. This includes safeguarding privacy, maintaining robust cybersecurity, ensuring data quality, and enabling interoperability across systems where appropriate. Data use shall be transparent, lawful, secure, and aligned with the broader public interest.

3.6. Institutions shall ensure equitable access to institutionally adopted AI-enabled systems and services, including reasonable accommodations for persons with disabilities.

AI-enabled systems and services shall be designed and deployed in a manner that ensures equitable access for all users, regardless of ability, language, or socio-economic background. Universities shall incorporate principles of inclusive and universal design, ensuring that digital platforms, tools, and services are accessible to persons with disabilities. Where necessary, reasonable accommodations and alternative pathways shall be provided to ensure full participation. This provision supports both legal compliance and the broader goal of inclusive education.

3.7. Universities shall invest in infrastructure, governance, and human capacity to support AI adoption.

Sustainable and effective AI adoption requires deliberate investment in three key areas:

- Infrastructure: reliable connectivity, computing resources, and data systems
- Governance: policies, oversight mechanisms, and risk management frameworks
- Human capacity: AI literacy, technical expertise, and leadership capability

Universities shall allocate resources strategically to build and maintain these enablers, ensuring that AI initiatives are scalable, secure, and aligned with institutional and national priorities. Such investments also support long-term competitiveness and innovation.

4. Policy Goals

The following goals describe the system-level outcomes this framework is designed to produce. Progress toward these goals will be monitored through the mechanisms set out in Section 8.9.

4.1. Universal Institutional Policy Adoption

Within two years of this framework's adoption, all state universities shall have developed and submitted to the UGC an institutional AI policy aligned with the minimum standards set out in this framework.

4.2. Governance Structures Established Across the Sector

Within two years of this framework's adoption, all state universities shall have designated a governance structure or responsible authority with explicit oversight of AI use, accountability, and compliance at the institutional level.

4.3. Baseline AI Literacy Across the University Community

Within three years of this framework's adoption, all state universities shall have implemented baseline AI literacy programmes covering responsible use, academic integrity, and data protection for students, academic staff, and administrative staff.

4.4. Equitable and Accessible AI Integration

AI-enabled systems and services deployed for student-facing or staff-facing institutional functions shall meet minimum accessibility standards, including compatibility with assistive technologies and, where relevant and feasible, functional adequacy across Sinhala, Tamil, and English.

4.5. Risk Governance Operational for High-Risk AI Systems and High-Stakes Decisions

All state universities shall have operational risk classification, procurement review, and human oversight mechanisms in place for AI systems classified as high-risk and for AI use in high-stakes institutional decisions, including admissions, assessment, progression, employment, and disciplinary processes, within two years of this framework's adoption.

4.6. Contribution to National AI Development

Sri Lanka's state universities shall be active contributors to the national AI ecosystem, including through locally relevant research, Sinhala- and Tamil-language AI resource development, and responsible industry and public-sector partnerships aligned with the AI Sri Lanka 2028: Sri Lanka's National Strategy on AI.

5. Applicability and Scope

This framework applies to all universities in the State University System of Sri Lanka, encompassing their academic, administrative, and research functions. It covers AI use across the following areas:

- teaching, learning, and assessment
- research and research support
- institutional decision-making and administrative services
- student- and staff-facing digital systems

The framework applies to all members of the university community, including students, academic staff, administrative staff, and institutional leadership, as well as external systems, vendors, and partnerships where AI systems are used in institutional processes. It addresses both the adoption of external AI tools and systems and the development or deployment of internally developed AI systems. The framework applies across varying levels of risk and impact, from routine academic use to high-stakes institutional decision-making, with governance expectations calibrated accordingly.

5.1. Institutionally Adopted AI Systems

Institutionally adopted AI systems—meaning systems integrated into university operations, decision-making, data processing, or student and staff services—are subject to the full governance, procurement, oversight, and compliance requirements of this framework. This includes systems procured from external vendors, systems developed internally, and systems introduced through research partnerships or donor-funded initiatives where the university assumes operational responsibility. The formal governance requirements set out in Section 8 apply in full to institutionally adopted systems. These include risk classification, human oversight in high-stakes contexts, documentation and auditability, procurement safeguards, and accountability mechanisms.

Illustrative example: A university that integrates an AI-enabled student analytics platform into its student information system is deploying an institutionally adopted system. It must conduct a risk assessment, assign governance responsibility, ensure data protection compliance, and establish mechanisms for human oversight and appeal before deployment.

5.2. Individual Use of Externally Available AI Tools

Individual use of externally available AI tools by students, academic staff, and administrative staff, for purposes such as learning, writing, research, teaching preparation, or routine administrative support, is already widespread across Sri Lanka's university sector and is not subject to the formal institutional governance requirements that apply to institutionally adopted systems.

Such use is instead governed through institutional guidance, academic integrity policies, ethical standards, and the applicable safeguards set out in Section 8.5 (Academic Practice, Integrity and Communication). Universities are expected to provide clear guidance to students and staff on responsible individual use, disclosure expectations, and the boundaries of acceptable AI assistance in academic and professional work.

Illustrative example: A student who uses a publicly available AI writing tool to revise an assignment, or a lecturer who uses such a tool to prepare teaching materials, is engaged in individual use governed by academic integrity and institutional guidance, rather than system-level procurement and risk governance.

5.3. The Boundary in Practice

The distinction between institutional and individual use is not always immediately obvious, and universities should apply judgment based on the following considerations. Use is more likely to be institutional in character where it involves university-procured or university-funded systems, integration with institutional data or platforms, use at scale across a faculty or administrative unit, or consequential

decisions affecting students or staff. Where uncertainty exists, universities should apply the governance expectations appropriate to the higher-risk classification.

Illustrative example: A department that procures access to an AI tool through institutional or faculty funding, integrates it into a shared workflow, and uses it to process student data is operating at the institutional level, even if individual staff members are the direct users.

6. Policy Implementation



6.1. Foundational Digital Infrastructure

Universities shall ensure that the responsible adoption of artificial intelligence is supported by reliable, secure, accessible, and sustainable digital infrastructure. AI-enabled systems cannot be implemented responsibly without adequate connectivity, computing capacity, data management, cybersecurity, platform governance, and technical support. These provisions establish the minimum infrastructure conditions required for credible AI adoption across state universities, while recognising that institutions differ in capacity, scale, mission, and readiness. Implementation may be phased according to institutional circumstances, provided that universities continue to work toward the minimum standards set out in this framework and do not deploy higher-risk AI systems without the necessary infrastructure, data governance, security, and oversight arrangements.

6.1.1. Minimum Infrastructure Readiness

Universities shall maintain a minimum level of digital infrastructure readiness before deploying AI systems in higher-risk academic, administrative, research, or student-facing contexts. This includes reliable connectivity, secure access controls, governed data systems, cybersecurity safeguards, appropriate technical support, and mechanisms for monitoring and review. Before deploying AI systems that may affect student progression, assessment, admissions, staff processes, research governance, or access to institutional services, universities shall ensure that the underlying digital environment is sufficiently reliable, secure, and auditable.

Illustrative example: Before deploying an AI-supported student progression or early-warning system, a university should ensure that the relevant student data is accurate and securely stored, access is properly controlled, the system can be monitored, and affected students have a pathway for human review.

6.1.2. Connectivity, Security, and Resilience

Universities shall maintain reliable network connectivity and secure digital access to support teaching, learning, research, administration, and student services involving AI-enabled tools or systems. Network

and platform access shall be protected through appropriate technical and administrative controls, including authentication, authorisation, access monitoring, backup arrangements, incident response, disaster recovery, and continuity planning. Where AI-enabled systems access institutional platforms, databases, or user accounts, universities shall ensure that these systems do not introduce avoidable cybersecurity risks or create unmanaged dependencies that could disrupt essential university functions.

Illustrative example: If an AI-enabled student service platform is connected to a student information system, the university should ensure secure authentication, defined access permissions, monitoring of unusual activity, and a clear process for responding to technical failures or security incidents.

6.1.3. Computing and Data Systems

Universities shall ensure access to computing and data management systems appropriate to their institutional needs and risk profile. These may include cloud services, on-premise systems, shared infrastructure, or hybrid arrangements. The choice of infrastructure shall be guided by security, sustainability, cost-effectiveness, institutional capacity, and the nature of the AI use case. Universities shall establish structured systems for storing, managing, securing, retrieving, and retaining institutional data used in teaching, research, administration, and student support. Data systems used for AI-enabled applications shall have clear responsibility for data quality, access control, retention, privacy, and protection.

Illustrative example: A university may rely on cloud-based computing for teaching and basic experimentation, while a research-intensive institution may invest in specialised computing infrastructure for AI model development, provided that both approaches meet relevant data protection and security requirements.

6.1.4. Platforms, Interoperability, and Accessibility

Universities shall maintain appropriate digital platforms for core university functions, including teaching, research, administration, and student services. Any AI-enabled integration with these platforms shall be subject to institutional review, particularly where it involves institutional data, student or staff records, or consequential decisions. Universities shall consider interoperability, portability, accessibility, and long-term sustainability when adopting AI-enabled systems. AI-related infrastructure should not create unnecessary fragmentation, vendor lock-in, or dependence on isolated platforms that cannot be maintained, integrated, audited, or replaced. AI-enabled platforms used for student- or staff-facing services shall be accessible and inclusive, including for persons with disabilities and, where relevant, for users working in Sinhala, Tamil, and English.

Illustrative example: When procuring an AI-enabled administrative system, the university should assess whether it can integrate with existing learning management, student record, HR, and finance systems, whether data can be exported if the system is replaced, and whether the service remains accessible to diverse users.

6.1.5. Shared Infrastructure, Common Standards, and Institutional Differentiation

The UGC shall encourage shared infrastructure, pooled expertise, common technical guidance, and sector-level support where these improve quality, cost-effectiveness, security, and equitable access across state universities. This may include shared platforms, common procurement templates, advisory standards, technical evaluation criteria, and coordinated capacity-building support. Universities may invest in advanced infrastructure according to their mission, capacity, and strategic priorities, including high-performance computing, AI laboratories, specialised data platforms, and advanced research environments. At the same time, all universities shall work toward the minimum infrastructure readiness required for responsible AI adoption.

Illustrative example: A university with strong AI research capacity may establish a high-performance computing facility, while another university may initially focus on reliable connectivity, secure platforms, governed data systems, and access to shared infrastructure.

6.1.6. Review and Continuous Improvement

Universities shall review the adequacy, security, accessibility, sustainability, and resilience of digital infrastructure supporting AI adoption at least annually. This review may be aligned with institutional IT planning, cybersecurity review, quality assurance, risk management, or strategic planning cycles. The review shall identify gaps in connectivity, computing capacity, cybersecurity, data governance, platform integration, accessibility, technical staffing, and support for higher-risk AI deployment. Where gaps are identified, universities shall prepare phased improvement plans that are proportionate to institutional capacity and risk. The UGC may use findings from institutional reviews, quality assurance processes, and sector-level monitoring to identify common infrastructure needs and support shared solutions across the state university system.

Illustrative example: A university may conduct an annual AI infrastructure readiness review through its IT, QA, and governance units, identify weaknesses in data storage or cybersecurity, and include corrective actions in its institutional development plan.

6.2. Risk-Based AI Governance

AI systems shall be governed using a lifecycle-based risk management approach aligned with international best practice, recognising that risk is contextual, dynamic, and evolving across design, development, deployment, use, monitoring, and decommissioning. Risk classification is not static and may change as system use, scale, deployment context, or potential harms evolve.

All institutionally adopted AI systems, and any individual or departmental use that materially involves institutional data, institutional platforms, scale deployment, or consequential decisions affecting students or staff, shall undergo risk classification prior to procurement, development, deployment, or use.

For the purposes of this framework, meaningful human oversight refers to the ability of appropriately authorised individuals to review, intervene in, override, and remain accountable for AI-supported decisions or processes. Human oversight shall be proportionate to the level of risk and potential impact associated with the AI system or context of use.

6.2.1. Risk Levels

6.2.1.1. Low Risk

AI systems with minimal potential for harm and limited impact on individuals or institutional decision-making.

- Typically support routine, low-stakes functions
- Risks are well understood and easily mitigated

Illustrative examples:

- AI-assisted grammar, translation, or writing-support tools used by students or staff for low-stakes drafting and revision
- Basic automated scheduling tools that do not materially affect workload, progression, accommodations, or access to required academic opportunities
- Basic chatbots that provide general campus information, such as office locations, opening hours, or navigation support

Governance expectation for institutionally adopted low-risk systems: basic transparency, proportionate documentation, and periodic review. Individual low-risk use of externally available AI tools remains governed by institutional guidance, academic integrity policies, and applicable disclosure expectations rather than formal system-level risk governance.

6.2.1.2. Moderate Risk

AI systems with meaningful but manageable impact, where outputs may influence decisions but are not solely determinative.

- Potential for bias or error exists but can be mitigated
- Context, scale, and user population significantly influence risk

Illustrative examples:

- AI tools that recommend academic courses or career pathways for student consideration
- AI-assisted grading tools used only as a secondary input to human assessment
- AI early-warning systems that flag students for possible academic support
- AI tools that help identify candidates for scholarships or bursaries, where final selection remains with a human committee

Governance expectation: Documented risk assessment, bias and performance testing, and defined human oversight.

6.2.1.3. High Risk

AI systems with significant potential to affect rights, safety, or life outcomes, particularly in high-stakes contexts.

Characteristics may include:

- errors or bias that may result in material harm or inequitable outcomes
- deployment in sensitive or regulated domains
- use in decisions with significant academic, financial, disciplinary, employment, or health consequences

Illustrative examples:

- AI systems used to support admissions, scholarship allocation, progression, or exclusion decisions
- AI-supported clinical, health, or treatment-related decision systems used in university clinical, research, training, or service contexts
- AI tools used to screen applicants for recruitment, promotion, or other employment-related decisions

AI systems used in high-stakes institutional decisions shall be treated as high-risk AI contexts and shall be subject to the corresponding governance, oversight, and accountability requirements set out in this framework. Governance expectations include pre-deployment validation, continuous monitoring, auditability, clear accountability, and meaningful human oversight with the ability to intervene.

6.2.1.4. Prohibited AI Use

AI uses that present unacceptable or unmitigable risk to rights, fairness, safety, academic integrity, or institutional accountability.

Characteristics may include:

- absence of meaningful human oversight in consequential decisions
- use of sensitive personal attributes or indicators in ways that unfairly restrict access, opportunity, support, or fair treatment
- deceptive, coercive, exploitative, or manipulative influence over students or staff
- intrusive or disproportionate surveillance without clear legal authority, institutional approval, necessity, and safeguards

Illustrative examples:

- AI systems that automatically admit, reject, grade, progress, discipline, or exclude a student without authorised human review and access to appeal.
- AI systems that assign risk scores, rankings, penalties, or access to opportunities based on sensitive indicators such as disability, ethnicity, religion, political opinion, language background, gender, or socio-economic status, where such use disadvantages, excludes, or stigmatises individuals or groups.

- AI systems that intentionally manipulate students or staff through deceptive, coercive, or exploitative design, especially where they exploit age, disability, economic vulnerability, or dependence on university services.

6.2.2. Lifecycle Governance

The lifecycle governance functions set out below are drawn from the NIST AI Risk Management Framework (AI RMF 1.0), an internationally recognised voluntary framework for managing AI-related risk, and are intended to work as an integrated cycle—establishing accountability structures, identifying and contextualising risk, evaluating that risk against measurable criteria, and implementing controls and monitoring to manage it on an ongoing basis.

6.2.2.1. Govern

Establish policies, structures, and accountability mechanisms to oversee AI use.

- Define roles, responsibilities, and oversight bodies
- Ensure alignment with ethical principles and legal requirements

Illustrative example: A university assigns oversight of high-risk AI systems to a designated governance committee, with defined approval, documentation, monitoring, and escalation procedures before deployment.

6.2.2.2. Map

Identify and contextualise risks associated with the AI system.

- Define intended purpose, users, and deployment context
- Identify potential harms and affected populations

Illustrative example: Before deploying an AI admissions support tool, the university identifies the affected applicants, data sources, decision points, and possible risks for students from different socio-economic, regional, or language backgrounds.

6.2.2.3. Measure

Assess and evaluate risks using appropriate metrics and testing.

- Test for bias, fairness, accuracy, and robustness
- Validate system performance against expected outcomes

Illustrative example: Before using an AI-assisted assessment tool, the university tests whether its outputs are accurate, consistent, and free from systematic bias across relevant student groups.

6.2.2.4. Manage

Implement mitigation strategies and ensure ongoing monitoring and improvement.

- Apply controls to reduce identified risks
- Monitor performance and respond to incidents

Illustrative example: An AI recruitment support tool is monitored after deployment, with audit logs reviewed and use suspended if biased or unreliable outcomes are detected.

6.2.3. Mandatory Risk Considerations

AI systems subject to risk classification under this framework shall be evaluated against the following cross-cutting considerations:

6.2.3.1. Fairness and Bias

AI systems shall be designed and tested to **minimise discriminatory outcomes**.

Illustrative example: An admissions support system is tested to ensure that it does not systematically disadvantage applicants from particular schools, regions, language backgrounds, or demographic groups.

6.2.3.2. Accessibility and Inclusion

AI systems shall be **usable and equitable across diverse populations**, including persons with disabilities.

Illustrative example: An AI-enabled student service system is reviewed for accessibility in Sinhala, Tamil, and English and for compatibility with assistive technologies such as screen readers.

6.2.3.3. Data Governance and Security

AI systems shall ensure **data quality, integrity, privacy, and protection**.

Illustrative example: A university health or counselling-related AI system uses securely stored data, defined access permissions, appropriate consent processes, and safeguards against unauthorised access.

6.3. Governance, Accountability and Safeguards

Universities shall ensure that the use of artificial intelligence is governed through appropriate structures, processes, and controls that uphold accountability, manage risk, and ensure compliance with ethical, legal, and institutional standards. These provisions establish the minimum requirements for oversight and assurance, enabling responsible and sustainable use of AI across institutional functions.

6.3.1. Institutional Accountability for AI Systems

Universities shall assign clear responsibility for the governance, oversight, compliance, and review of AI systems to designated institutional authorities. Accountability for outcomes shall remain with identifiable human authorities. Institutions shall maintain appropriate documentation, records, and review mechanisms for AI systems used in academic, administrative, research, or decision-making contexts, particularly where systems are classified as moderate- or high-risk.

Auditability shall include, where appropriate:

- documentation of system purpose, scope, and intended use
- records of data sources, procurement, and governance approvals
- documentation of human oversight and decision-making processes
- mechanisms for reviewing system outputs, performance, and reported concerns

Institutions shall establish internal review and audit processes aligned with the level of risk and impact associated with the AI system. The UGC may integrate AI governance review into existing quality assurance, compliance, or institutional review processes where appropriate.

Illustrative example: A university may designate a Deputy Vice Chancellor or a senior committee to oversee AI governance, with defined responsibility for ensuring compliance, monitoring, and institutional review across faculties and administrative units.

6.3.2. Governance Structures and Internal Oversight

Universities shall establish or designate appropriate governance structures to oversee AI use, including policy development, monitoring, and review functions. These may include existing bodies such as Senates, Quality Assurance units, Ethics Review Committees, and Boards of Management.

Illustrative example: A university may integrate AI oversight into its Centre for Quality Assurance and Senate subcommittees, with Ethics Review Committees providing oversight for research-related AI use.

6.3.3. Monitoring, Audit, and Compliance Mechanisms

Universities shall implement mechanisms to monitor AI use, maintain records, and enable internal and external audit of compliance with institutional and UGC requirements. Monitoring mechanisms should include procedures for reporting, documenting, and responding to AI-related incidents, errors, or harms in proportion to the level of risk involved.

Illustrative example: Institutions may maintain registers of AI systems in use and periodically review high-risk applications through internal audit or quality assurance processes.

6.3.4. Legal and Ethical Compliance

Universities shall ensure that the use of AI complies with applicable legal, regulatory, and ethical standards, including requirements related to data protection, privacy, and academic integrity.

Illustrative example: An AI system used for student analytics shall comply with national data protection legislation and institutional policies governing the use of personal data.

6.3.5. Resourcing for Governance and Safeguards

Universities shall allocate adequate financial, technical, and human resources to support governance structures, risk management processes, and oversight mechanisms for AI use.

Illustrative example: Institutions may allocate dedicated staff or budget lines to support AI governance functions, including training, monitoring, and compliance activities.

6.3.6. Inclusive Governance and Accessibility Oversight

Universities shall ensure that governance and risk management processes include oversight of accessibility and inclusion, including the potential impact of AI systems on persons with disabilities and other vulnerable groups.

Illustrative example: Governance bodies may include accessibility considerations in risk assessments and review processes, ensuring that AI systems do not create barriers for users with disabilities.

6.4. Institutional Decision-Making and Services

Universities shall ensure that the use of artificial intelligence in high-stakes institutional decisions and consequential institutional services is aligned with principles of fairness, transparency, accountability, and due process. These provisions apply to contexts that materially affect the rights, opportunities, or experiences of students and staff, including admissions, assessment, human resource processes, and student- or staff-facing services.

6.4.1. Human Oversight in High-Stakes Decisions

Universities shall ensure meaningful human oversight in all high-stakes decisions involving AI, where the responsible person or body has sufficient information, time, and authority to review, modify, or reverse the AI-assisted recommendation. AI systems shall not be used as the sole basis for such decisions. Universities shall require prior governance approval before deploying AI in high-stakes decision contexts and shall ensure that the authority to suspend an AI-assisted decision pending review is available where risks are substantiated. Where an AI-influenced decision is found to be erroneous or unfair, universities shall have a mechanism to correct or redress that decision in a timely manner.

Illustrative example: An AI system may assist with ranking applicants for admission, but final decisions are reviewed and confirmed by an authorised academic or administrative body with authority to modify, reject, or suspend the AI-assisted recommendation.

6.4.2. Transparency of AI Use

Universities shall ensure that the use of AI in decision-making processes and services is disclosed in a clear and accessible manner where such use may materially influence outcomes, institutional processes, or user experience. Affected persons shall be informed, where appropriate, of the role AI plays in the process and of available mechanisms for human review.

Illustrative example: Where AI is used to assist in large-scale assessment, students shall be informed of its use, its role in the evaluation process, and the process through which they may seek clarification or review.

6.4.3. Right to Explanation and Appeal

Universities shall ensure that individuals affected by AI-supported decisions have access to appropriate explanations and to timely, effective mechanisms for human review, appeal, correction, and redress.

Illustrative example: A student may request an explanation and human review of an assessment outcome where AI has been used in marking, grading, or progression-related decision-making.

6.4.4. Fairness and Non-Discrimination

Universities shall take reasonable measures to identify, monitor, and mitigate bias in AI-supported decision-making and services, ensuring equitable treatment across individuals and groups.

Illustrative example: A university using AI to support recruitment, admissions, assessment, progression, or selection reviews outcomes to ensure that particular groups are not disadvantaged on the basis of language, socio-economic status, disability, gender, ethnicity, religion, or other protected or sensitive characteristics.

6.4.5. Documentation and Auditability

Universities shall maintain appropriate documentation, decision records, and audit trails of AI-supported decision-making and services to enable internal oversight, external quality assurance, review, appeal, and accountability.

Illustrative example: For an AI-supported admissions or recruitment process, the university maintains records of the system used, the AI output, the human review undertaken, and the final decision.

6.4.6. Accessibility and Reasonable Accommodation

Universities shall ensure that AI-supported decisions and services are accessible to persons with disabilities and that reasonable accommodations are provided where required, in accordance with applicable legal and policy frameworks.

Illustrative example: AI-enabled student services shall be designed to be compatible with assistive technologies, and alternative access pathways shall be provided where necessary.

6.5. Academic Practice, Integrity and Communication

UNIVERSITY GRANTS COMMISSION

6.5.1. System-wide AI Vocabulary and Glossary

The UGC shall develop, maintain, and facilitate the continuous refinement of a system-wide baseline glossary for AI-related terms.

Illustrative example: Defining common terms such as “generative AI,” “hallucination,” “human-in-the-loop,” and “AI-assisted writing” so that all universities interpret them consistently in academic policies.

6.5.2. Shared Standards for AI Use and Integrity

The UGC shall require all institutions to adopt a shared system-wide vocabulary and baseline standards for AI use, authorship, and academic integrity.

Illustrative example: Universities adopt a shared disclosure rule requiring students and staff to state when AI has materially assisted academic work, while clarifying that AI systems cannot be credited as authors.

6.5.3. Minimum Standards for Transparency and Fairness

The UGC shall develop and maintain minimum standards governing transparency, accountability, fairness, and human oversight in the institutional use of AI systems, particularly in high-stakes academic and administrative contexts.

Illustrative example: Establishing a national requirement that AI-assisted grading or assessment processes remain explainable, reviewable, and subject to meaningful human oversight.

6.5.4. System Coordination and Consistency

The UGC shall support system-level coordination across institutions through guidance, model frameworks, implementation support, and mechanisms for inter-university collaboration and knowledge sharing.

Illustrative example: The UGC issues advisory guidance on AI-assisted plagiarism detection so that universities apply such tools consistently, cautiously, and with appropriate human review.

6.5.5. Integration into Quality Assurance

The UGC shall integrate AI-related considerations into existing quality assurance frameworks.

Illustrative example: Including AI-use policies as part of institutional quality audits conducted by QA units.

6.5.6. Good Practice and Knowledge Sharing

The UGC may publish non-binding companion guidance, model policy outlines, implementation checklists, approved practice notes, and examples of existing institutional policies to support universities in developing context-appropriate AI policies. Such resources are intended to provide practical support and promote system-level coherence, without requiring universities to adopt a single uniform template.

Illustrative example: A university in the early stages of developing its institutional AI policy may consult a UGC-issued model outline and adapt its section on academic integrity disclosures to reflect faculty-specific practices, without being required to replicate the model in full.

UNIVERSITIES

6.5.7. Academic Integrity and Responsibility

Universities shall ensure that students, faculty, and researchers remain fully responsible for the originality, accuracy, and ethical integrity of all academic work, regardless of AI use.

Illustrative example: A student who uses a generative AI tool to draft or revise an assignment remains responsible for verifying sources, correcting errors, and ensuring that the final submission represents their own work.

6.5.8. Human Oversight in High-Stakes Academic Decisions

Universities shall ensure that AI use in high-stakes academic decisions includes meaningful human review and final human accountability.

Illustrative example: AI-assisted grading recommendations must be reviewed and confirmed by an academic before final marks are released.

6.5.9. Transparency of AI Use

Universities shall implement clear disclosure of AI use in academic work and communication.

Illustrative example: Students include a brief declaration in assignments or theses stating whether AI tools were used and, where relevant, how they supported the work.

6.5.10. Redress and Appeal Mechanisms

Universities shall establish formal appeal and redress mechanisms for AI-influenced academic decisions, including decisions related to assessment, grading, academic integrity, plagiarism detection, authorship, and suspected misconduct. AI detection tools, including tools used to detect AI-generated writing, plagiarism, authorship irregularities, or academic misconduct, shall not be used as the sole basis for an adverse academic decision. Any finding of academic misconduct involving AI-assisted detection shall require human review, contextual assessment of the student's work, consideration of relevant evidence, and access to a fair appeal or redress process.

Illustrative example: A student whose work is flagged by an AI-supported plagiarism or AI-writing detector is not penalised solely on the basis of the tool's output. The case is reviewed by an authorised academic or committee, the student is given an opportunity to respond, and the final decision is based on the full academic context and available evidence.

6.5.11. Adoption and Contextual Extension of Standards

Universities shall adopt the system-wide baseline glossary and standards and extend them contextually at the university, faculty, and departmental levels.

Illustrative example: A Faculty of Computing may add discipline-specific rules for AI code generation while retaining the UGC baseline definitions and disclosure expectations.

6.5.12. Curriculum and Pedagogical Adaptation

Universities are expected to ensure that curricula and teaching practices are adapted for an AI-enabled academic environment.

Illustrative example: A course replaces a purely factual recall task with an assignment requiring students to evaluate, verify, and improve AI-generated outputs using course concepts.

6.5.13. Alignment and Compliance with UGC Standards

Universities shall align institutional AI policies, procedures, and governance mechanisms with applicable UGC standards and shall monitor implementation through existing institutional governance and quality assurance processes.

Illustrative example: University quality assurance committees periodically reviewing faculty or departmental AI-related policies and practices to ensure alignment with national UGC requirements and institutional procedures.

6.6. Capacity, Literacy and Implementation

UNIVERSITY GRANTS COMMISSION

6.6.1. AI Literacy Standards (Baseline Definition & Maintenance)

The UGC shall define and maintain baseline AI literacy standards to ensure a system-wide minimum level of safe, ethical, and informed AI use.

Illustrative example: The UGC baseline requires students and staff to understand responsible AI use, bias, privacy, academic integrity, and the limits of AI-generated outputs.

6.6.2. System-wide Implementation and Monitoring

The UGC shall facilitate, monitor, and integrate AI literacy implementation into national quality assurance frameworks.

Illustrative example: AI literacy compliance becomes part of university QA audits and annual reporting.

6.6.3. Knowledge Sharing and Capacity Building Ecosystem

The UGC shall facilitate a coordinated learning ecosystem by enabling sharing of expertise, training materials, and pilot outcomes across institutions.

Illustrative example: A university-developed AI literacy module is shared through a UGC-supported repository so that other institutions can adapt it to their own contexts.

6.6.4. Recognition and Incentives for Good Practice

The UGC shall establish recognition frameworks to reward institutions that demonstrate impactful and innovative AI practices.

Illustrative example: The UGC recognises institutions that demonstrate well-documented, inclusive, and responsible AI practices, such as accessible training, strong governance, and evidence of student support.

UNIVERSITIES

6.6.5. AI Literacy Implementation and Training

Universities shall implement AI literacy and training programmes that meet UGC baseline standards.

Illustrative example: First-year students complete an introductory AI literacy module covering responsible use, academic integrity, privacy, bias, and appropriate disclosure.

6.6.6. Continuous Updating of AI Capacity

Universities shall regularly review and update AI capacity-building programmes to reflect technological change.

Illustrative example: AI training modules are updated annually to include new tools and practices.

6.6.7. Human Oversight and Institutional Capability

Universities shall develop institutional capacity for human oversight of AI, ensuring staff can evaluate and audit AI-assisted high-stakes decisions.

Illustrative example: Academic staff are trained to review AI-assisted grading outputs, identify possible errors or bias, and retain responsibility for final marks.

6.6.8. Inclusive and Accessible AI Learning

Universities shall ensure AI literacy and capacity building are inclusive and accessible to diverse learner needs.

Illustrative example: AI literacy materials are provided in accessible formats and, where feasible, in Sinhala, Tamil, and English.

6.6.9. Reporting and Accountability to UGC

Universities shall provide periodic progress updates to the UGC on AI literacy and implementation.

Illustrative example: Each university submits an annual report on AI training participation and outcomes.

6.6.10. Multilingual and Contextual Capacity Building

Universities shall progressively strengthen multilingual capacity building and develop context-specific AI training beyond baseline standards, taking into account institutional capacity, learner needs, and available resources.

Illustrative example: AI workshops use Sinhala, Tamil, and English examples and include discipline-specific scenarios from teaching, research, administration, and student services.

6.6.11. Institutional Flexibility in Delivery

Institutions may determine methods, curricula, and delivery mechanisms for AI literacy, provided baseline standards are met.

Illustrative example: One university uses online modules, another uses blended workshops, both meeting the same standard.

6.6.12. Role of Staff Development Centres

University Staff Development Centres (SDCs) are encouraged to lead the design and delivery of AI training programmes.

Illustrative example: SDCs run regular AI-upskilling sessions for academic staff across faculties.

6.7. Data, Systems and Procurement

Universities shall ensure that the acquisition, deployment, and use of AI-related systems are governed through responsible data governance, secure digital infrastructure, and transparent procurement practices. These provisions establish minimum expectations for the protection of student, staff, institutional, and research data, while enabling universities to adopt AI systems in ways that are locally relevant, legally compliant, secure, and sustainable.

6.7.1. Data Governance Review Before AI Deployment

Universities shall ensure that AI-related systems involving student, staff, institutional, or research data undergo appropriate risk classification and data governance review before adoption or deployment.

Illustrative example: Before adopting an AI-enabled student analytics platform, a university reviews what student data will be used, who will have access to it, where the data will be processed, and what safeguards are in place.

6.7.2. Protection of Sensitive and Institutional Data

Universities shall not permit sensitive institutional data, student data, staff data, or protected research data to be used for AI training, fine-tuning, testing, or external processing without appropriate legal, ethical, technical, and institutional review.

Illustrative example: A university does not upload identifiable student performance records or staff records to an external AI platform unless the use has received appropriate privacy, consent, data protection, and institutional risk review.

6.7.3. Procurement Safeguards for AI Systems

Universities shall ensure that procurement processes for AI-related systems include assessment of privacy, cybersecurity, data retention, access control, auditability, accountability, interoperability, explainability where relevant, and long-term platform dependency.

Illustrative example: When procuring an AI-enabled learning platform extension, the university assesses integration, data export, access control, auditability, vendor obligations, and long-term dependency before approval.

6.7.4. Vendor and Partner Accountability

Universities shall not enter into arrangements that grant vendors or collaborators broad, unclear, unrestricted, or undisclosed rights to use university data, student data, staff data, or research data for model development, commercial reuse, or secondary purposes, unless such use has been explicitly reviewed, approved, documented, and subjected to appropriate legal, ethical, technical, and institutional safeguards.

Illustrative example: A contract with an AI service provider should state who is responsible if student data is exposed, how incidents must be reported, and how the university can retrieve or delete its data when the service is discontinued.

6.7.5. Limits on Secondary Use of University Data

Universities shall permit secondary use of university data, student data, staff data, or research data for model training, fine-tuning, testing, analytics, commercial development, research, or service improvement only where such use is purpose-specific, documented, lawful, proportionate, and subject to appropriate approval, consent or notice where required, data protection safeguards, and institutional oversight.

Illustrative example: A vendor providing an AI chatbot for student services should not be allowed to use student queries or institutional records to train commercial models unless this has been explicitly reviewed and approved.

6.7.6. Documentation and System Registers

Universities shall maintain appropriate documentation for significant AI systems, including their purpose, data sources, responsible units, vendor or partner details, risk assessment, review status, and mechanisms for escalation, review, suspension, or discontinuation.

Illustrative example: A university may maintain an internal register of AI systems used in teaching, administration, research support, and student services, with additional review requirements for systems involving sensitive data or higher-risk functions.

6.7.7. Local Relevance and Language Considerations

Universities shall take reasonable steps to ensure that AI systems used in teaching, learning, administration, research, or student support are appropriate to the Sri Lankan higher education context, including language, accessibility, disciplinary needs, and institutional capacity.

Illustrative example: An AI-enabled student advisory system should be assessed for whether it can support students appropriately in Sinhala, Tamil, and English, and whether its recommendations are suitable for the local university context.

6.7.8. Shared Infrastructure and Pooled Expertise

The UGC shall encourage shared infrastructure, common technical resources, inter-university collaboration, and pooled expertise where these improve security, cost-effectiveness, quality, and equitable access across the state university system.

Illustrative example: Universities may use common procurement templates, shared technical evaluation criteria, or sector-level expertise when assessing AI systems that are likely to be used across multiple institutions.

6.7.9. Alignment with Legal and Institutional Requirements

Universities shall ensure that AI-related procurement, data use, system deployment, and partnership arrangements comply with applicable national laws, regulations, and institutional governance requirements. This includes the Personal Data Protection Act, No. 9 of 2022, as amended by the Personal Data Protection (Amendment) Act, No. 22 of 2025, cybersecurity requirements, public procurement rules, research ethics requirements, and institutional policies on data access, retention, confidentiality, consent, accountability, and responsible use. Where AI systems involve the collection, processing, sharing, storage, transfer, or reuse of personal data relating to students, staff, research participants, or other university stakeholders, universities shall ensure that such processing is lawful, transparent, purpose-specific, proportionate, and subject to appropriate safeguards. Particular care shall be taken where AI systems involve sensitive data, large-scale data processing, automated profiling, cross-border data flows, external vendors, or secondary use of university data for model training, testing, fine-tuning, or commercial development.

Illustrative example: Before deploying an AI system that processes student, staff, research participant, or student service data, the university reviews compliance with data protection law, consent requirements, access controls, retention rules, vendor obligations, and accountability mechanisms.

6.8. Innovation, Partnerships and Funding

Universities shall promote AI-related research, development, innovation, partnerships, and funding in ways that advance national development, academic excellence, public-interest values, and responsible use of technology. These provisions enable universities to engage with industry, donors, public institutions, and international collaborators while maintaining safeguards for academic integrity, data protection, institutional autonomy, transparency, and system-wide equity. All AI-related innovation, partnership, and funding arrangements shall comply with the risk governance, data protection, procurement, accountability, and monitoring requirements set out in this framework.

6.8.1. Promotion of AI Research and Innovation

Universities shall recognise AI-related research, development, and innovation as important functions of the state university system and pursue them in ways aligned with educational, scientific, and national development priorities.

Illustrative example: A university may support AI research in agriculture, health, education, engineering, public administration, or environmental management where such work responds to national needs and advances public benefit.

6.8.2. Responsible Partnership Governance

Universities shall ensure that AI-related partnerships, pilots, and externally supported initiatives are subject to appropriate institutional review and approval processes.

Illustrative example: Before entering into an AI partnership with an industry or international partner, a university should review the proposal for academic integrity, data governance, conflicts of interest, transparency, public-interest value, and long-term sustainability.

6.8.3. Safeguards for High-Impact Innovation Initiatives

Universities shall ensure that AI-related innovation initiatives involving significant student or staff data, consequential institutional decisions, or externally imposed operational dependency do not proceed without governance review and documented accountability.

Illustrative example: A donor-funded AI system for student progression monitoring is reviewed for data use, student notice, accountability, human oversight, and the university's ability to suspend or discontinue the system.

6.8.4. Assessment of Risks and Benefits in Collaborations

Universities shall assess proposed AI collaborations not only for technical or financial value, but also for local relevance, long-term sustainability, institutional autonomy, and the fair distribution of risks and benefits.

Illustrative example: A no-cost AI platform partnership is reviewed for hidden costs, data access conditions, dependency risks, and whether benefits extend beyond a small group of users.

6.8.5. Multi-University Collaboration and Shared Platforms

The UGC shall encourage multi-university collaboration, shared platforms, responsible experimentation, and joint development of locally relevant AI resources, particularly where pooled effort can reduce cost, improve quality, and strengthen national impact.

Illustrative example: Several universities may collaborate to develop Sinhala- and Tamil-language datasets, shared research infrastructure, or common AI training resources rather than duplicating the same effort independently.

6.8.6. Equitable Access to Funding and Innovation Opportunities

The UGC shall encourage funding mechanisms that support equitable participation across institutions, including universities with lower existing capacity, so that AI innovation does not become concentrated only in already advantaged settings.

Illustrative example: A national AI funding call may encourage joint proposals between institutions with advanced AI capacity and institutions that are beginning to build their AI capability.

6.8.7. Commercialisation, Entrepreneurship, and Intellectual Property

Universities may pursue commercialisation, entrepreneurship, and intellectual property development arising from AI-related work, provided such activity remains consistent with academic values, public-interest commitments, legal requirements, and institutional policies.

Illustrative example: A university research team may commercialise an AI tool developed through academic research, provided that ownership, benefit-sharing, student contribution, research ethics, and public-interest obligations are properly addressed.

6.8.8. Transparency in Material Partnership Arrangements

Universities shall ensure transparency in material partnership arrangements that affect institutional autonomy, access to data, research direction, long-term platform dependency, or public-interest commitments.

Illustrative example: If an external partner funds an AI laboratory or platform, the university should clearly document the partner's role, data access rights, expected outputs, intellectual property arrangements, and any influence over research direction.

6.8.9. Local Language and Context-Sensitive AI Resources

Universities are encouraged to support the development of locally relevant AI resources, including Sinhala- and Tamil-language assets, domain-specific datasets, and context-sensitive applications that serve Sri Lanka's needs.

Illustrative example: A university consortium may develop AI resources for Sinhala and Tamil academic writing support, local public-service applications, or discipline-specific datasets relevant to Sri Lankan agriculture, health, education, or industry.

6.8.10. Alignment with Public Interest and National Priorities

Universities shall ensure that AI-related innovation, partnerships, and funding arrangements remain aligned with public interest, academic integrity, legal and ethical standards, and national development priorities.

Illustrative example: An externally funded AI initiative is assessed not only for financial or technical benefit, but also for educational value, national relevance, institutional independence, and responsible AI use.

6.9. Monitoring, Evaluation and Adaptation

The UGC and universities shall ensure that the implementation of this policy framework is subject to ongoing monitoring, evaluation, and periodic review, in order to support continuous improvement, accountability, and responsiveness to technological, institutional, and societal change.

6.9.1. Monitoring and Evaluation

Universities shall establish mechanisms to monitor and evaluate the implementation of this framework, including the following areas:

6.9.1.1. Compliance with Framework Standards

Institutions shall demonstrate adherence to the minimum requirements set out in this framework, including governance, accountability, and safeguards in AI-supported decision-making and services.

Illustrative example: An internal review verifies that high-stakes AI-supported decisions include documented human oversight, notice to affected persons, and accessible appeal mechanisms.

6.9.1.2. Infrastructure Readiness

Institutions shall assess and maintain the adequacy of digital infrastructure required to support responsible and effective use of AI systems.

Illustrative example: A university may evaluate whether its learning management systems and administrative platforms can support secure, auditable AI integration.

6.9.1.3. Capacity Development

Institutions shall monitor the development of institutional capacity, including staff training, technical expertise, and organisational readiness for AI adoption and governance.

Illustrative example: Staff Development Centres may track participation in AI training programmes and assess competency development across academic and administrative staff.

6.9.1.4. Accessibility and Inclusion Outcomes

Institutions shall evaluate whether AI-enabled systems and services are accessible and inclusive, including for persons with disabilities and across Sinhala, Tamil, and English language contexts.

Illustrative example: A university conducts user testing to confirm that AI-enabled student services are accessible to persons with disabilities and usable across Sinhala, Tamil, and English contexts.

6.9.1.5. Innovation, Institutional Effectiveness, and Public Value

Institutions shall assess how the use of AI contributes to institutional effectiveness, responsible innovation, educational quality, public value, and national development.

Illustrative example: Universities may evaluate improvements in administrative efficiency or student support services resulting from responsible AI adoption.

6.9.2. Quality Assurance and System-Level Oversight

The UGC shall integrate monitoring of this policy framework into its existing quality assurance and institutional review processes.

- Compliance and implementation shall be assessed through institutional and programme reviews conducted by the Quality Assurance Council of the UGC.
- Findings from these processes shall inform system-level guidance, capacity-building initiatives, and policy refinement.
- Where significant implementation gaps, governance failures, or non-compliance with minimum standards are identified, the UGC may require institutions to develop corrective action plans and undertake appropriate follow-up measures.

Illustrative example: AI-related practices in admissions or assessment may be examined during programme reviews to ensure alignment with standards on fairness, transparency, and human oversight.

6.9.3. Review Cycle

The UGC shall undertake a **formal review of this policy framework every three (3) years**, aligned with national policy and quality assurance cycles.

This review shall assess:

- Effectiveness of implementation across institutions
- Emerging risks and challenges
- Adequacy of safeguards and governance mechanisms
- Alignment with national priorities and international developments

Illustrative example: A system-level review may identify gaps in accessibility or auditability and recommend updated standards or guidance.

6.9.4. Continuous Improvement and Adaptive Updates

Between formal review cycles, the UGC may issue updates, refinements, guidance, or clarifications as necessary based on:

6.9.4.1. Technological Change

Developments in AI technologies that introduce new capabilities, risks, or use cases

Illustrative example: The emergence of more advanced automated decision systems may require updated expectations for human oversight.

6.9.4.2. Risk Assessments

Identification of new or evolving risks, including those affecting fairness, transparency, and inclusion

Illustrative example: Detection of bias in AI-supported recruitment processes may trigger updated safeguards.

6.9.4.3. Stakeholder Feedback

Inputs from students, staff, institutional leadership, and external partners

Illustrative example: Student feedback on AI-assisted assessment identifies the need for clearer explanations, improved review procedures, or stronger safeguards against unfair outcomes.

6.9.4.4. Quality Assurance Findings

Evidence and recommendations arising from institutional and programme reviews conducted by the UGC

Illustrative example: Recurrent issues identified across multiple institutions may lead to the issuance of system-wide guidance or clarifications.

6.9.5. Interim Guidance, Clarifications, or Advisories

The UGC may issue **interim guidance, clarifications, or advisories** to address emerging issues without requiring full policy revision as and when required.

7. Glossary

A

Accessibility

The design and delivery of AI systems, services, and digital environments to ensure usability by individuals with diverse abilities, including persons with disabilities.

Accountability (Institutional Accountability)

The assignment of clear responsibility to identifiable individuals or institutional bodies for the governance, oversight, decisions, and outcomes of AI use.

Algorithmic Bias

Systematic and unfair differences in AI system outputs that result in discriminatory or inequitable outcomes across individuals or groups.

Artificial Intelligence (AI)

Machine-based systems capable of performing tasks that typically require human intelligence, including prediction, classification, recommendation, decision support, and content generation.

AI Lifecycle

The full set of stages through which an AI system passes, including design, development, testing, deployment, use, monitoring, and decommissioning.

AI Literacy

The knowledge, skills, and critical understanding required to use, evaluate, and interact with AI systems safely, effectively, and ethically.

AI System

A machine-based system that generates outputs (e.g., predictions, recommendations, decisions, or content) influencing real or virtual environments.

Auditability

The capacity for AI-supported systems, decisions, and governance processes to be reviewed, documented, traced, and evaluated through appropriate institutional mechanisms.

Automated Profiling

The use of an AI system or automated process to evaluate, classify, predict, rank, or infer characteristics, behaviour, performance, risk, or needs of an individual or group.

B

Bias Mitigation

Measures implemented to detect, reduce, and manage bias in AI systems across design, data, and deployment stages.

C

Capacity Building / Capacity Development

The process of developing institutional skills, infrastructure, governance mechanisms, and human expertise required for responsible AI adoption and oversight.

Compliance

Adherence to UGC framework standards, institutional policies, and applicable legal, regulatory, and ethical requirements.

Context of Use

The specific environment, purpose, scale, and user population within which an AI system operates, influencing its risk profile.

Continuous Improvement

An ongoing process of refining policies, systems, and practices based on monitoring, evaluation, feedback, and emerging risks or technologies.

Continuous Monitoring

Ongoing evaluation of AI system performance, behaviour, and risk after deployment.

Cross-Border Data Flow

The transfer, storage, access, or processing of data outside Sri Lanka, including through cloud services, external vendors, international collaborators, or platforms hosted in another jurisdiction.

Cybersecurity

The protection of systems, networks, and data from unauthorised access, attack, disruption, or misuse.

D**Data Governance**

The framework of policies, processes, and controls governing data collection, access, quality, integrity, use, sharing, and protection.

Data Protection

Legal and technical safeguards ensuring personal and sensitive data is processed lawfully, securely, and ethically.

Data Protection Review

A documented institutional review of whether personal or sensitive data used in an AI system is collected, processed, stored, shared, transferred, or reused lawfully, securely, transparently, and for a legitimate purpose.

Data Security

Measures implemented to prevent unauthorised access, breaches, or misuse of data.

Decision Support System (AI-supported)

An AI system that provides recommendations or analysis to assist human decision-making but does not replace human authority.

Digital Infrastructure

The systems, networks, platforms, and computing resources required to support digital operations and AI deployment.

Documentation (AI Systems)

Records describing an AI system's purpose, design, data sources, functioning, risk classification, and role in decision-making.

E**Equity**

The principle of ensuring fair access, treatment, and outcomes across individuals and groups, accounting for differences in need and context.

Explainability

The extent to which the internal logic or outputs of an AI system can be understood and communicated in human-interpretable terms.

F**Fairness and Non-Discrimination**

The principle that AI systems should not result in unjustified or systemic disadvantage to individuals or groups.

G**Generative AI**

A category of artificial intelligence systems capable of producing new content—including text, images, audio, code, and data—by learning patterns from large datasets.

Govern (Function)

The establishment of policies, roles, responsibilities, and oversight mechanisms to ensure accountable and ethical AI use.

Governance (AI Governance)

The structures, processes, and policies used to direct, control, and oversee AI systems and their impacts.

Governance Structures

Institutional bodies (e.g., Senate, QA units, Ethics Review Committees) responsible for AI oversight and compliance.

H**Hallucination**

The generation of outputs by an AI system that are plausible in appearance but factually incorrect, fabricated, or unsupported by any reliable source.

High-Risk AI System

An AI system with significant potential to affect safety, rights, or life outcomes, requiring stringent governance, validation, and oversight.

High-Stakes Decision

A decision that significantly affects the rights, opportunities, or outcomes of students or staff (e.g., admissions, grading, employment).

Human Oversight (Meaningful Human Oversight)

Active human review and control over AI outputs, including authority to validate, modify, or override decisions.

Human-in-the-Loop

A governance approach in which human judgment is integrated into AI decision-making processes.

I**Incident Response**

Processes for detecting, reporting, managing, and resolving failures, risks, or harms arising from AI systems.

Inclusion

Ensuring AI systems are designed and deployed to accommodate diverse populations, including linguistic, socio-economic, and ability-based differences.

Inclusive Design

The proactive design of systems to be usable by the widest range of users without the need for adaptation.

Individual Use of Externally Available AI Tools

The use of publicly available or personally accessed AI tools by students, academic staff, administrative staff, or researchers for learning, writing, teaching preparation, research support, or routine work, where the tool is not formally procured, integrated, or adopted by the university.

Infrastructure Readiness

The availability and adequacy of digital systems and technical capacity required for responsible AI deployment.

Institutionally Adopted AI System

An AI system that is procured, funded, developed, approved, integrated, or operationally used by a university for teaching, research, administration, decision-making, data processing, or student and staff services.

Interoperability

The ability of systems and platforms to exchange, integrate, and use data effectively.

L**Legal and Ethical Compliance**

Adherence to applicable laws, regulations, ethical standards, and institutional policies governing AI use.

Lifecycle-Based Risk Management

A continuous approach to identifying, assessing, and managing risks across all stages of the AI lifecycle.

Low-Risk AI System

An AI system with minimal potential for harm and limited impact on individuals, institutional decision-making, or access to rights, opportunities, or services. Low-risk systems typically support routine, low-stakes functions and require proportionate governance such as basic transparency, documentation where appropriate, and periodic review.

M**Manage (Function)**

The implementation of risk mitigation strategies, monitoring, and response mechanisms.

Map (Function)

The process of identifying an AI system's purpose, stakeholders, risks, and deployment context.

Material Partnership Arrangement

A partnership, collaboration, funding arrangement, pilot, service agreement, or external engagement that may affect university data, institutional autonomy, research direction, intellectual property, student or staff services, long-term platform dependency, or public-interest obligations.

Measure (Function)

The evaluation of AI system performance, including testing for accuracy, bias, reliability, and robustness.

Moderate-Risk AI System

An AI system with meaningful but manageable impact requiring oversight, testing, and human supervision.

Monitoring and Evaluation (M&E)

Processes used to assess performance, compliance, and impact of AI systems and policy implementation.

Multilingual Accessibility

The ability of systems to function effectively across Sinhala, Tamil, and English contexts.

P**Personal Data**

Any information relating to an identified or identifiable individual, including students, staff, research participants, applicants, alumni, or other persons connected to university functions.

Privacy

The right of individuals to control how their personal data is collected, used, and shared.

Procurement (AI Systems)

The process of acquiring AI tools or services, including evaluation of technical, legal, ethical, and operational considerations.

Prohibited AI Use

AI applications that pose unacceptable risks or violate ethical, legal, or institutional standards.

Q**Quality Assurance (QA) Integration**

The incorporation of AI governance and safeguards into institutional and UGC quality assurance processes.

R**Reasonable Accommodation**

Adjustments or modifications made to ensure persons with disabilities can participate equally in AI-enabled environments.

Redress Mechanism

Formal processes allowing individuals to challenge, appeal, or seek remedy for AI-supported decisions.

Risk (AI Context)

The combination of the likelihood and severity of harm arising from AI system use.

Risk Classification

The categorisation of AI systems into defined levels (e.g., low, moderate, high, prohibited) based on potential impact.

Risk Mitigation

Measures taken to reduce the likelihood or severity of harm.

Resourcing (Sustainable Resourcing)

Allocation of adequate financial, technical, and human resources to support AI implementation and governance.

S**Secondary Use of Data**

The use of data for a purpose different from the purpose for which it was originally collected, including reuse for model training, fine-tuning, testing, analytics, commercial development, research, or service improvement.

Sensitive Data

Personal data or institutional data that requires heightened protection because its misuse may create legal, ethical, financial, reputational, academic, or personal harm. This may include health data, disability-related data, biometric data, demographic data, disciplinary records, academic performance data, employment records, financial information, research participant data, or confidential institutional records.

Severity of Harm

The extent of negative impact resulting from an AI system's outputs or decisions.

System-Level Oversight

Monitoring, evaluation, and coordination conducted by the UGC across institutions.

T**Transparency**

The clear disclosure of when, how, and why AI is used, including its role in decision-making processes.

U

User Population

The group of individuals interacting with or affected by an AI system, including students, staff, and external stakeholders.

V

Vendor Lock-In

A situation in which a university becomes dependent on a particular vendor, platform, system, data format, infrastructure, or service arrangement in ways that make transition, replacement, interoperability, data export, or institutional control difficult or costly.

8. References

National

AI Sri Lanka 2028: Sri Lanka's National Strategy on AI

Government of Sri Lanka (Committee to Formulate an AI Strategy – CFSAI), 2024.

Sri Lanka's National Strategy on Artificial Intelligence (AI Sri Lanka 2028).

Available at: https://mode.gov.lk/assets/files/National_AI_strategy_Annexes-a07a4000e1cb01b59a67dcf0dae77f15.pdf

Sets out Sri Lanka's national strategy for responsible AI development and adoption through 2028.

National Digital Economy Strategy 2030

Information and Communication Technology Agency (ICTA), Government of Sri Lanka, 2023.

National Digital Economy Strategy 2030.

Available at: <https://www.icta.lk/icta-assets/uploads/2023/05/Annex-1-National-Digital-Strategy-2030.pdf>

Provides the overarching digital transformation framework aligned with AI adoption and economic development.

Personal Data Protection Act, No. 9 of 2022, as amended by the Personal Data Protection (Amendment) Act, No. 22 of 2025

Parliament of the Democratic Socialist Republic of Sri Lanka, 2022 and 2025.

Personal Data Protection Act, No. 9 of 2022; Personal Data Protection (Amendment) Act, No. 22 of 2025.

Available at: https://www.documents.gov.lk/view/act/2025/10/22-2025_E.pdf

Provides Sri Lanka's legal framework for the processing and protection of personal data, including the amendments introduced in 2025.

Protection of the Rights of Persons with Disabilities Act, No. 28 of 1996, as amended (Sri Lanka)

Parliament of Sri Lanka, 1996 (as amended).

Protection of the Rights of Persons with Disabilities Act, No. 28 of 1996.

Available at: http://www.commonlii.org/lk/legis/num_act/potropa28o1996334/

Provides legal protections relating to the rights, access, and non-discrimination of persons with disabilities in Sri Lanka.

International

NIST AI Risk Management Framework (AI RMF 1.0)

National Institute of Standards and Technology (NIST), U.S.A., 2023.

Artificial Intelligence Risk Management Framework (AI RMF 1.0).

Available at: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

A voluntary framework providing guidance for managing risks across the AI lifecycle.

UNESCO Recommendation on the Ethics of Artificial Intelligence

United Nations Educational, Scientific and Cultural Organization (UNESCO), 2021.

Recommendation on the Ethics of Artificial Intelligence.

Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000380455>

Global normative framework promoting ethical, human-rights-based AI.

OECD AI Principles

Organisation for Economic Co-operation and Development (OECD), 2019.

OECD Principles on Artificial Intelligence.

Available at: <https://oecd.ai/en/ai-principles>

Internationally endorsed principles for trustworthy AI, including transparency, fairness, and accountability.

UN Convention on the Rights of Persons with Disabilities (CRPD)

United Nations, 2006.

Convention on the Rights of Persons with Disabilities.

Available at: <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html>

Provides a global human rights framework for disability inclusion and accessibility.

European Union Artificial Intelligence Act

European Parliament and Council of the European Union, 2024.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Official Journal of the European Union, L 2024/1689, 12 July 2024.

Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

Provides a comprehensive risk-based regulatory framework for AI systems, including provisions on prohibited AI practices, high-risk AI systems, transparency obligations, human oversight, AI literacy, accessibility, environmental protection, and innovation support.

Institutional**UGC Quality Assurance Framework**

University Grants Commission (UGC), Sri Lanka.

Quality Assurance Framework for Sri Lankan Universities.

Available at: <https://eugc.ugc.ac.lk/qac/>

Defines standards and processes for quality assurance across higher education institutions.

AI Policy Working Group Outputs

University Grants Commission (UGC) AI Policy Working Group, Sri Lanka, 2025–2026.

Draft Outputs and Policy Development Documents (Unpublished/Internal).

(Internal policy development materials; not publicly available online)

9. AI Policy Framework Development Team

CONSULTANT AND TEAM LEAD

- Prof. Usree Bhattacharya, Associate Professor in TESOL and World Languages, Language and Literacy Education Department, University of Georgia, U.S.A.

GROUP A - GOVERNANCE, INSTITUTIONS AND OPERATIONS

- Prof. Vajira H. W. Dissanayake, Chair and Senior Professor of Anatomy, Genetics and Biomedical Informatics, Faculty of Medicine, University of Colombo (Group Leader)
- Prof. Thushara Weerawardena, Chair Professor of Electronic & Telecommunication, Department of Electrical, Electronic & Telecommunication Engineering, Faculty of Engineering, General Sir John Kotelawala Defence University
- Prof. Lasith Gunawardena, Professor and Head of the Department of Information Technology, Faculty of Management Studies & Commerce, University of Sri Jayewardenepura
- Dr. Asanka Sayakkara, Senior Lecturer at the University of Colombo School of Computing, University of Colombo

GROUP B - PEOPLE, PRACTICE, AND CAPABILITY

- Prof. Uthayasanker Thayasivam, Head, Department of Computer Science and Engineering, University of Moratuwa (Group Leader)
- Prof. Hiran Amarasekera, Professor in Forestry and Environment Science, Faculty of Science, University of Sri Jayewardenepura
- Dr. Chathura Rajapaksha, Senior Lecturer, Department of Industrial Management, University of Kelaniya Sri Lanka
- Mr. Malintha Perera, Senior Lecturer, Department of Accountancy, Faculty of Commerce and Management Studies, University of Kelaniya

GROUP C - SYSTEMS, INFRASTRUCTURE, AND ECOSYSTEM

- Prof. Roshan Ragel, Professor in Computer Engineering, Faculty of Engineering, University of Peradeniya (Group Leader)
- Prof. Hiran Jayaweera, Professor in Physics, Department of Physics, Faculty of Science, University of Colombo
- Dr. Ajantha Atukorale, Director and Senior Lecturer in Computer Science, University of Colombo School of Computing
- Dr. Upul Jayasinghe, Senior Lecturer, Department of Computer Engineering, Faculty of Engineering, University of Peradeniya

INSTITUTIONAL AND EMBASSY SUPPORT

- Prof. Kapila Seneviratne, UGC Chairman
- Professor K L Wasantha Kumara, UGC Vice Chairman
- Dr. Janadari Wijesinghe, Head of Academic Affairs, University Grants Commission
- Dr. Steven Walter, Public Diplomacy Officer, U.S. Embassy, Colombo
- Ms. Aruni Peiris, Coordinator English Language Programs, U.S. Embassy, Colombo

PUBLICATION INFORMATION

National Policy Framework for the Use of Artificial Intelligence in the State University System of Sri Lanka



University Grants Commission | Sri Lanka | 2026