

AI AND ADVANCED DIGITAL TECHNOLOGIES GOVERNANCE POLICY

POLICY OVERVIEW

Abu Dhabi University (ADU) is committed to the responsible, secure, and effective use of Artificial Intelligence (AI) and advanced digital technologies to support evidence-based decision-making, improve operational efficiency, enhance service delivery, and advance institutional excellence.

Resolution No	
Executive Order	
Supersedes	
Version Number:	
Date Approved:	
Effective Date:	
Policy Owner:	
Viewing Access Level:	
Next Review Date:	

Change History

Version Number	Change Description	Date	Changed By
01	▪ New Policy		

1. Introduction

The University shall adopt an institution-wide approach to digital transformation. AI and advanced digital technologies shall be governed responsibly and should be integrated, monitored, and continuously improved to support measurable value across academic and administrative functions.

2. Policy Statement

This policy establishes the principles, governance arrangements, roles, controls, and performance expectations for the selection, development, procurement, implementation, use, monitoring, and evaluation of AI and advanced digital technologies at Abu Dhabi University.

The policy aims to ensure that digital initiatives align with institutional priorities, improve the quality and accessibility of services, support informed decision-making, reduce manual work and duplication, integrate effectively with relevant systems and processes, protect data privacy and cybersecurity, and are evaluated against measurable outcomes.

3. Scope

This policy applies to all Abu Dhabi University colleges, campuses, departments, administrative units, faculty members, staff, students, contractors, consultants, and service providers involved in the development, procurement, management, integration, operation, or use of AI and advanced digital technologies.

The policy applies to technologies including artificial intelligence, generative AI, AI agents, intelligent automation, predictive analytics, decision-support systems, Internet of Things devices, smart-campus technologies, robotic process automation, integrated enterprise systems, digital workflows, electronic approvals, electronic signatures, chatbots, digital service platforms, learning analytics, AI-enabled educational technologies, identity-management systems, single sign-on platforms, and other emerging technologies that may enhance institutional performance.

4. Definitions

Term	Definition
Artificial Intelligence	Computer-based systems capable of performing tasks that normally require human intelligence, including generating content, recognizing patterns, making predictions, supporting decisions, or automating responses.
Advanced Digital Technologies	Technologies used to improve institutional performance through automation, intelligence, connectivity, analytics, and digital service delivery, including AI, IoT, analytics, robotic process automation, and related tools.
Generative AI	AI systems that create or produce content such as text, images, audio, video, software code, or other outputs based on prompts, data, or instructions.
AI Agent	A software-based system that can perform tasks, make recommendations, or take actions with varying levels of autonomy based on defined objectives, rules, data, or user instructions.
High-Impact Decision	A decision that may significantly affect an individual's rights, status, opportunities, obligations, or access to services, or materially affect the University's legal, financial, academic, or operational position.
Human Oversight	Review, supervision, validation, or intervention by an authorized person to ensure that AI-supported or automated activities are appropriate, accurate, lawful, and consistent with university requirements.
Personal Data	Any information relating to an identified or identifiable individual, including student, employee, applicant, alumni, contractor, or other stakeholder information protected under applicable law or university policy.
Sensitive Information	Information classified by the University as confidential, restricted, regulated, or otherwise requiring enhanced protection due to legal, contractual, security, academic, operational, or reputational risk.
Data Owner	The individual or unit accountable for the quality, classification, access, use, protection, and governance of a specific dataset or information domain.

Process Owner	The individual or unit accountable for the design, performance, control, and improvement of a business or academic process supported by digital technologies.
----------------------	---

5. Guiding Principles

Principle	Requirement
Strategic Alignment	AI and advanced digital technology initiatives shall support university strategy, institutional priorities, academic quality, and operational needs.
Institutional Integration	Digital solutions should be interoperable, scalable, and integrated with relevant university systems and processes wherever appropriate and feasible.
Human Accountability	AI and automated systems should support human decision-making. Accountability for decisions shall remain with the authorized individual or unit.
Responsible and Ethical Use	Technologies shall be used fairly, transparently, inclusively, and responsibly. Appropriate measures should be taken, where feasible, to reduce risks related to bias, inaccurate outputs, discrimination, and unintended consequences.
Privacy and Security	Technologies shall comply with applicable legal requirements and university policies relating to data protection, confidentiality, cybersecurity, identity management, and access control.
Measurable Value	Digital initiatives should be evaluated against defined or available performance indicators, including, where applicable, impact on service quality, efficiency, cost-effectiveness, user experience, and decision-making.
Continuous Improvement	Digital technologies should be reviewed and enhanced over time based on available performance data, stakeholder feedback, emerging risks, and technological developments.

6. Governance and Accountability

The implementation of this policy shall be overseen through Abu Dhabi University's relevant governance structures for AI, digital transformation, operational excellence, information technology, data governance, privacy, risk management, compliance, cybersecurity, and internal audit, as applicable and as these structures mature.

Major initiatives involving institutional data, personal data, high-impact decisions, integration with core systems, external technology providers, or significant financial investment shall be subject to appropriate review and approval through the relevant governance, legal, risk, privacy, cybersecurity, procurement, and operational channels where applicable and before implementation where required.

Responsible Party	Key Responsibilities
University Leadership	Approve strategic priorities, major investments, and high-impact initiatives where required; support alignment of AI and digital initiatives with institutional strategy and governance expectations.

AI Steering Committee	Review major AI and digital initiatives where applicable; promote responsible innovation; monitor institutional impact over time; support the development of appropriate controls, approvals, and review mechanisms.
Digital Advancement, Transformation and AI Function	Identify opportunities in collaboration with departments; coordinate implementation; support technical feasibility, system integration, cybersecurity, identity and access management, business continuity, vendor assessment, and operational support where applicable.
Data Owners and Process Owners	Support data quality, appropriate classification, lawful use, controlled access, accurate reporting, process effectiveness, and available evidence of performance and control implementation.
Colleges and Administrative Units	Identify business and academic needs; participate in design and implementation; support adoption within their areas; monitor results where feasible; maintain available evidence of impact and issues.
Risk, Compliance, Privacy, Cybersecurity, and Internal Audit Functions	Review relevant risks, controls, compliance requirements, privacy implications, cybersecurity requirements, and available audit evidence for applicable initiatives.
Users	Use university-provided systems and approved external technologies responsibly; validate outputs; protect confidential information; comply with this policy; report concerns, incidents, errors, or inappropriate use.

7. Areas of Application

AI and advanced digital technologies may be used across academic, administrative, operational, and strategic functions where their use is lawful, secure, responsible, and aligned with university priorities.

Area	Examples of Appropriate Application
Student Services	Admissions, registration, advising, student support, engagement, financial assistance, career services, and communication.
Teaching, Learning, and Academic Administration	Teaching support, curriculum development, academic advising, scheduling, assessment moderation, learning analytics, faculty support, and quality assurance.
Institutional Decision-Making	Dashboards, analytics, forecasting, risk monitoring, resource allocation, institutional performance management, and decision-support tools.
Human Resources	Recruitment, onboarding, employee services, workforce planning, performance management, professional development, and engagement.

Finance and Procurement	Budgeting, approvals, procurement workflows, expenditure monitoring, contract management, reporting, and audit trails.
Facilities, Assets, and Smart-Campus Operations	Campus safety, energy efficiency, preventive maintenance, asset management, classroom utilization, laboratory utilization, and facilities planning.
Research and Innovation	Research support, data analysis, innovation, and interdisciplinary collaboration, subject to research ethics, confidentiality, intellectual-property, and publication requirements.
Administrative Workflows	Secure digital approvals, electronic signatures, paperless processes, automated workflows, and traceable service delivery.

8. Responsible Use of Artificial Intelligence

Users shall review and verify AI-generated content, recommendations, analyses, and outputs before using them for official purposes. AI-generated outputs shall not be presented as final, authoritative, or verified unless they have been appropriately reviewed by an authorized person.

AI-generated recommendations shall not be used as the sole basis for high-impact decisions, including decisions relating to admissions, student progression, assessment, employment, disciplinary matters, financial decisions, legal matters, regulatory matters, or other decisions with significant implications for individuals or the University. Such decisions shall remain subject to appropriate human oversight and accountability.

Units using AI systems should take reasonable measures, where feasible, to assess accuracy, fairness, bias, relevance, and reliability. Identified concerns should be documented, escalated, and addressed through the appropriate process owner, data owner, or governance channel.

9. Permitted, Restricted, and Prohibited Use

9.1 Permitted Use

AI and advanced digital technologies may be used for approved academic, administrative, operational, analytical, communication, research, and service-delivery purposes where the use is lawful, secure, transparent where required, consistent with university policy, and subject to appropriate review and accountability.

9.2 Restricted Use

The following uses require prior review and approval through the relevant university governance, legal, risk, privacy, cybersecurity, procurement, and operational processes where applicable: processing personal data or sensitive information; integrating AI tools with university systems; deploying AI agents or automations that take action on behalf of users; using AI to support high-impact decisions; using external AI platforms for university work; procuring AI-enabled products or services; and using AI for research involving confidential, regulated, or personal data.

9.3 Prohibited Use

Users must not use AI or advanced digital technologies to disclose confidential, restricted, regulated, or sensitive institutional information through unauthorized external platforms; bypass cybersecurity, access-control, procurement, vendor-assessment, records-management, or data-governance requirements; generate or present misleading records, evidence, academic work, research outputs, or official communications; make high-impact decisions without human oversight; or engage in unlawful, deceptive, discriminatory, unethical, or policy-inconsistent activity.

10. Privacy, Consent, and Lawful Data Use

Where AI or advanced digital technologies involve the collection, use, analysis, sharing, storage, profiling, or other processing of personal data, such processing shall be lawful, fair, transparent, necessary, proportionate, and consistent with applicable legal and regulatory requirements and related university policies.

Individuals shall be provided with appropriate notice regarding the use of their personal data, including, where relevant, the purpose of processing, the nature of the technology being used, and any material impact on decisions affecting them. Where required by applicable law or policy, appropriate consent or another valid legal basis for processing shall be established before personal data is processed.

Where AI-generated outputs, recommendations, profiling, or automated processing materially influence decisions relating to individuals, the relevant unit shall ensure appropriate human oversight, transparency, and review mechanisms, with documentation maintained where available or required.

11. Data Governance

Data used in AI systems, dashboards, automation tools, and digital platforms shall be managed in accordance with university data-governance requirements. Data owners shall be identified for major institutional datasets where applicable and shall support data accuracy, currency, classification, validation, lawful use, and protection against unauthorized access or disclosure.

Access to data shall be role-based and limited to authorized users. Systems should retain appropriate logs, approvals, and audit trails where available or required. Data-sharing arrangements with external parties shall be governed through appropriate contractual, privacy, cybersecurity, and institutional controls.

12. Cybersecurity and Business Continuity

AI and advanced digital technologies shall comply with applicable university information-security, identity-management, access-control, vendor-security, and business-continuity requirements. Appropriate controls may include secure authentication, single sign-on where applicable, role-based access controls, encryption, secure data transmission, security updates, vulnerability assessment, risk monitoring, backup and recovery arrangements, incident reporting, vendor-security assessments, periodic access reviews, and monitoring of connected devices and systems.

Systems supporting critical operations should have documented recovery procedures where applicable and should be included in relevant business-continuity and incident-response arrangements as these arrangements mature.

13. Integration and Interoperability

Abu Dhabi University shall prioritize secure, scalable, and interoperable solutions that support coordinated workflows, data exchange, and reporting across relevant systems. Preference should be given to integrated platforms and reusable capabilities, where feasible, rather than isolated tools that duplicate data, create operational fragmentation, or increase support complexity.

Where appropriate and feasible, systems may integrate with student-information systems, learning-management systems, enterprise-resource-planning systems, human-resource systems, finance and procurement systems, facilities and asset-management systems, identity-management and single sign-on platforms, institutional dashboards and reporting tools, and digital communication and service platforms.

14. Performance Monitoring and Evidence

Each major initiative should have defined objectives, success measures, accountable owners, implementation records, and performance indicators where available and aligned with its intended outcomes.

Relevant process owners should review performance periodically where feasible and take corrective action where initiatives do not deliver expected value or where risks, errors, adoption issues, or control gaps are identified.

Performance indicators may include reduction in processing time, reduction in manual steps, reduction in paperwork, service-response time, user-adoption rates, user-satisfaction levels, reduction in errors, cost savings or cost avoidance, system uptime and reliability, number of integrated systems, number of automated workflows, student-engagement and retention indicators, space-utilization improvements, energy savings, compliance with service-level agreements, and optimization of digital resource usage.

Documentation and evidence may include, where available, approved plans and procedures, risk and privacy assessments, vendor assessments, integration diagrams, workflow records, electronic approval logs, performance reports, key performance indicators, user-adoption statistics, satisfaction surveys, training records, service-level reports, audit trails, before-and-after process comparisons, improvement plans, and records of corrective action.

15. Continuous Evaluation and Improvement

Abu Dhabi University should periodically review and enhance AI and advanced digital technologies based on available performance data, service-level results, stakeholder feedback, cybersecurity and privacy risks, AI accuracy and reliability, emerging technologies, institutional priorities, and regulatory developments.

Duplicated, outdated, underperforming, insecure, or unsupported systems should be reviewed and, where appropriate, enhanced, replaced, consolidated, or retired over time. Improvements and measurable outcomes should be documented where evidence is available.

16. Training and Awareness

Abu Dhabi University should provide appropriate training and awareness activities to support the effective, secure, and responsible use of AI and advanced digital technologies. Training may address AI literacy, responsible AI use, data privacy, confidentiality, cybersecurity, interpretation of dashboards and analytics, process automation, digital-service platforms, academic integrity, incident reporting, and role-specific obligations.

17. Compliance and Incident Reporting

All members of the university community and relevant external service providers shall comply with this policy and related university policies. Any inappropriate use, security concern, data breach, privacy concern, material system error, inaccurate AI output used for official purposes, or suspected policy violation shall be reported through the appropriate university channels.

Non-compliance may result in corrective, contractual, administrative, or disciplinary action in accordance with applicable university policies, contracts, laws, and regulations.

18. Policy Review

This policy shall be reviewed periodically and updated as required to reflect changes in legislation, regulatory requirements, university strategy, institutional priorities, technology developments, emerging risks, operational experience, performance-monitoring results, and stakeholder feedback.

19. Related policies and documents which form an integral part of this Policy

- ADU Personal data protection and privacy policy.
- ADU Sustainable Investment Policy.
- ADU Sustainability Strategic Plan.
- ADU Code of Conduct and Ethics.
- ADU Procurement and Purchasing Policy.

Exceptions

For any conditions/circumstances and/or exceptions outside the conditions stated in this policy, a request shall be presented to the Board of Directors for decision.

Authorization

This policy was authorized by the **University Chancellor**.