Strathmore University

Centre for Intellectual Property and Information Technology Law

Artificial Intelligence (AI) Policy for the Judiciary of Kenya.

Contents

Abbreviations

AI – Artificial Intelligence

AIGC - AI Governance Committee

ICT – Information Communication and Technology

JSC – Judicial Service Commission

JAIIA - Judicial AI Impact Assessment

JTF - Judiciary Transformation Framework

KJA – Kenya Judiciary Academy

ODPC – Office of the Data Protection Commissioner

SJT - Sustaining Judiciary Transformation Framework

STAJ - the Social Transformation through Access to Justice Blueprint

Definitions

AI Governance Committee (AIGC)	The body responsible for providing oversight, approval, and monitoring of AI systems deployed within the Judiciary.
AI Lifecycle	The stages through which an AI system progresses including design, development, procurement, testing, deployment, monitoring, maintenance, and decommissioning.
AI System	A software-based or integrated system that uses artificial intelligence techniques to generate outputs such as predictions, recommendations, classifications, or analyses that influence administrative or judicial processes.
Algorithmic Bias	Systematic and unfair discrimination produced by an AI system due to biased training data, flawed design, or improper deployment that results in unequal or discriminatory outcomes.
Artificial Intelligence (AI)	Computer-based systems designed to perform tasks that typically require human intelligence, including learning, reasoning, pattern recognition, natural language processing, and decision-support functions.
Cybersecurity	The practice of protecting systems, networks, data, and digital infrastructure from unauthorized access, cyberattacks, disruption, or misuse through technical, administrative, and legal safeguards.
Data Protection Impact Assessment (DPIA)	A risk assessment conducted to evaluate the potential impact of data processing activities on the privacy and rights of individuals, in accordance with applicable data protection laws.
Decision-Support System	An AI-enabled tool designed to assist judicial officers or staff by providing analysis, recommendations, or insights without replacing human decision-making authority.
Generative AI	Artificial intelligence systems capable of producing content such as text, images, audio, code, or other outputs based on prompts, training data, or user inputs.

High-Risk AI System	An AI system whose operation may significantly affect legal rights, judicial processes, or access to justice and therefore requires enhanced oversight, safeguards, and monitoring.
Human Oversight	The active supervision of AI systems by qualified personnel to ensure that automated outputs are reviewed, interpreted, and validated before being relied upon in decision-making or administrative processes.
Judicial AI Impact Assessment (JAIIA)	A structured assessment conducted prior to the deployment of an AI system to evaluate its potential impacts on constitutional rights, judicial independence, fairness, privacy, and access to justice.
Judicial Data	Any information generated, processed, or stored by the Judiciary while performing its functions, including case records, pleadings, judgments, internal communications, and administrative data.
Sensitive Judicial Information	Confidential or restricted information relating to court proceedings, judicial deliberations, parties to cases, or internal administrative processes within the Judiciary.
Third-Party AI Tools	AI systems or services developed and operated by external vendors or providers and accessed through external platforms, software applications, or cloud-based systems.
Vendor / Technology Partner	Any third-party entity that develops, supplies, maintains, or provides AI systems, services, or technical support to the Judiciary.

Chapter 1: Introduction

1.1 Background and Rationale

Since the adoption of the Constitution, the Judiciary has embarked on extensive transformation to enhance access to justice and uphold the rule of law. Anchored in Article 159, these reforms have been guided by three key blueprints: the Judiciary Transformation Framework (JTF), the Sustaining Judiciary Transformation (SJT) Framework, and the Social Transformation through Access to Justice (STAJ) Blueprint. Despite the progress achieved, challenges such as case backlogs and lengthy adjudication processes persist, affecting efficiency and public trust.

The adoption of Artificial Intelligence (AI) represents the next phase in the digital evolution. Globally, courts are increasingly deploying AI tools ranging from document analysis, speech-to-text transcription, and case scheduling to predictive analytics to accelerate proceedings, enhance decision-making, and promote transparency. AI can support STAJ's mandate by:

a. **Addressing backlog:** automating case triage and scheduling - AI can alleviate delays by automating case triage and dynamically scheduling hearings, freeing judicial officers to focus on substantive matters.

b. **Enhancing accuracy:** detecting inconsistencies and reducing human error - Machine learning can assist by scanning legal databases, identifying inconsistencies, and flagging errors, leading to more reliable judgments.

c. **Streamlining transcription:** automating court proceedings records - AI-powered speech-to-text technologies can convert oral submissions into written text in real time, reducing administrative workload and ensuring accurate records.

d. **Supporting research and analysis:** reviewing judgments and identifying trends - AI can rapidly process case law and legal commentary to identify trends, enabling evidence-based decisions and policy formulation.

e. **Reaching underserved communities:** deploying virtual legal assistants - AI-powered chatbots can provide accessible guidance, assisting individuals who cannot afford legal representation and bridging the justice gap.

f. **Bolstering public trust:** promoting transparency and data-driven decision-making - AI systems can enable data-driven tracking of case progress and publish anonymized dashboards, supporting a fairer and more accountable judicial system.

1.2 Scope

This Policy provides a structured framework for the introduction, management, and monitoring of AI within the Judiciary. It applies broadly to the adoption and governance of AI, covering diverse use cases including case allocation and analytics, AI-assisted chatbots, document review tools, transcription systems, and predictive modelling platforms. The Policy is directed at all key stakeholders: judges, magistrates, Kadhis, tribunal members, registrars, judicial staff, ICT professionals, Judicial Service Commission, the AI Governance Committee, judicial officers, the ICT Directorate, the Kenya Judiciary Academy, and all third-party partners.

This Policy operates within Kenya's existing legal and policy frameworks, notably the Constitution of Kenya (2010), the Data Protection Act (2019), the Judicial Service Act (2011), and the Computer Misuse and Cybercrimes Act (2018). It serves as a comprehensive framework for responsible AI adoption, acting as a reference point for judicial officers, a compliance roadmap for technology vendors, and a practical blueprint for planning, procuring, deploying, and auditing AI tools.

1.3 Constitutional Anchors

The deployment of AI in the Judiciary shall be firmly anchored in the Constitution of Kenya. Key provisions include:

a) **Article 10 – National values and principles of governance:** AI shall embody national values, including human dignity, equity, inclusivity, transparency, and accountability.

b) **Article 31 – Right to privacy:** The Judiciary shall ensure AI systems handling court records comply fully with data protection obligations, maintaining strict confidentiality.

c) **Article 48 – Access to justice:** AI systems should simplify procedures and improve efficiency, not create digital exclusion. Courts shall consider the needs of persons with disabilities and those with limited technological literacy.

d) **Article 50 – Fair hearing and judicial discretion:** AI tools may assist in research but shall never replace judicial reasoning. Human oversight shall remain central to all adjudicative processes.

e) **Article 159 – Judicial authority and use of technology:** The responsible use of AI aligns with the mandate to adopt technology, provided it strengthens judicial independence and upholds constitutional values.

f) **Article 160 – Independence of the judiciary:** AI tools shall operate strictly as support systems. The Judiciary shall retain full control over AI systems, including their data, algorithms, and outputs, to prevent external interference.

1.4 The STAJ Blueprint

Under the Social Transformation through Access to Justice (STAJ) Blueprint, digital transformation is guided by key principles:

a) **Efficiency:** Using AI to allocate resources effectively, reduce case backlogs, and streamline workflows.

b) **Prudence:** Leveraging data analytics for enhanced budget planning, performance monitoring, and institutional sustainability.

c) **Partnerships:** Collaborating with technology providers, academia, and civil society to co-design ethical and inclusive AI systems.

d) **Transparency:** Ensuring AI tools are explainable, auditable, and open to scrutiny to foster public trust.

e) **Social Transformation:** Ensuring digital innovation contributes to accessible, inclusive, and equitable justice for all, bridging existing inequalities.

1.5 Key Risks and Responsibilities

While the integration of AI presents immense opportunities, it also introduces new responsibilities and potential risks that shall be managed carefully. The deployment of AI within a constitutional and human rights framework demands vigilance to ensure that technology enhances, rather than undermines, the principles of fairness, accountability, transparency, and judicial independence.

Key risks in the integration of AI in the Judiciary include:

a) **Data privacy threats:** AI systems often rely on vast datasets containing personal or sensitive information. Without strong data governance, there is a risk of unauthorized access or re-identification, infringing on constitutional privacy rights under Article 31.

b) **Cybersecurity vulnerabilities:** The integration of AI expands the digital surface vulnerable to attacks such as hacking, data poisoning, or model manipulation, which could compromise the integrity of court data.

c) **Bias and discrimination:** AI tools can unintentionally reproduce or amplify societal biases present in historical data, posing a serious risk to constitutional guarantees of equality and fair hearing.

d) **Automation risks:** Excessive reliance on AI may dilute judicial autonomy. The Judiciary shall maintain a clear boundary between administrative automation and adjudicative discretion, ensuring AI serves as a decision-support tool, not a decision-maker.

To mitigate the risks associated with the adoption and use of Artificial Intelligence, the Judiciary shall undertake the following responsibilities:

a) **Ensure robust data protection and privacy safeguards:** The Judiciary shall implement strong data governance frameworks to protect personal and sensitive information processed by AI systems.

b) **Strengthen cybersecurity and system resilience:** The Judiciary shall implement robust cybersecurity measures to protect AI systems and judicial data from threats such as hacking, data poisoning, or system manipulation.

c) **Prevent algorithmic bias and discrimination:** The Judiciary shall take proactive measures to detect, prevent, and mitigate algorithmic bias in AI systems.

d) **Preserve judicial autonomy and human oversight**: The Judiciary shall ensure that AI systems operate strictly as decision-support tools and do not replace judicial reasoning or discretion. Judicial officers shall retain ultimate authority over all decisions, and clear safeguards shall be maintained to prevent undue reliance on automated systems.

Chapter 2: Guiding Principles for AI Adoption

The integration of Artificial Intelligence within the Judiciary shall be guided by a set of core principles that reflect the institution's constitutional mandate and its commitment to justice. These principles establish the foundational values that shall inform all decisions relating to the development, procurement, deployment, and use of AI systems within the Judiciary. Their purpose is to ensure that technology strengthens, rather than undermines, the integrity, fairness, transparency, and accessibility of the judicial process.

The principles outlined in this chapter provide an ethical and operational framework to guide responsible AI adoption. They serve as a common standard for evaluating all AI initiatives, ensuring alignment with the principles of legality, fairness, accountability, and respect for fundamental rights.

These guiding principles apply throughout the lifecycle of AI systems used within the Judiciary, from initial conception and procurement to deployment, monitoring, and eventual decommissioning. They are binding on all judicial officers, staff, and third-party vendors involved in the design, development, supply, or use of AI tools in support of judicial functions.

2.1 Policy Direction on Foundational Principles

It is the policy of the Judiciary that all AI systems and tools shall be developed, procured, and used in strict adherence to the principles outlined in this chapter. These principles are non-negotiable and shall serve as the primary benchmark for the AI Governance Committee when evaluating, approving, or rejecting any AI-related proposal. Any AI initiative that cannot demonstrate alignment with these principles shall be prohibited.

2.2 The AI Guiding Principles Framework

The following foundational principles shall guide AI adoption in the Judiciary, as detailed in **Appendix A: AI Guiding Principles Framework**:

a) **Legality and Trustworthiness:** All AI systems utilised by the Judiciary shall operate in a lawful, secure, and trustworthy manner, fully aligned with the Constitution of Kenya and applicable statutory frameworks.

b) **Inclusivity and Accessibility:** AI tools shall be developed and implemented in a people-centered and inclusive manner that promotes equitable access to justice, with particular attention to marginalized and vulnerable groups.

c) **Fairness and Bias Prevention:** The Judiciary shall prevent and mitigate algorithmic bias to ensure that AI systems operate fairly and do not produce discriminatory outcomes against any individual or group.

d) **Transparency and Explainability:** The use of AI shall be transparent, and systems shall be designed to provide clear, understandable explanations of their outputs to enable effective human oversight.

e) **Human Oversight and Accountability:** Judicial officers shall retain ultimate authority and responsibility over all decisions supported by AI systems.

f) **Security and Reliability:** AI systems shall incorporate robust security measures to protect against cyber threats in compliance with the Computer Misuse and Cybercrimes Act (2018) and applicable cybersecurity standards.

g) **Judicial Independence:** AI systems shall not undermine judicial autonomy and shall operate in a manner that respects the independence of the Judiciary as guaranteed under Article 160 of the Constitution.

h) **Efficiency and Sustainability:** AI shall enhance case management and resource allocation while ensuring that efficiency gains do not compromise fairness, due process, or the quality of justice.

i) **Locally Led:** AI tools shall reflect the needs and contexts of the communities served by the Judiciary, prioritizing locally developed or locally validated innovations and ensuring that data is stored and managed within Kenya where appropriate.

Chapter 3: Governance and Institutional Structure

Effective governance is essential to the responsible adoption and use of Artificial Intelligence within the Judiciary. This chapter establishes the institutional framework for the oversight of AI initiatives, ensuring that their development and deployment remain accountable, transparent, and aligned with constitutional values. It defines the roles and responsibilities of key institutions and actors within the Judiciary, while reinforcing that human judgment and judicial discretion remain central to the administration of justice.

The governance framework outlined in this chapter provides clear lines of authority, accountability, and coordination for all AI-related activities. Its purpose is to ensure that AI initiatives are designed, approved, and implemented in a structured, principled, and controlled manner, consistent with the Judiciary's legal mandate and ethical obligation.

3.1 Policy Direction on Governance and Institutional Structure

It is the policy of the Judiciary that all AI initiatives shall be subject to multi-tiered oversight. The AI Governance Committee (AIGC) shall provide strategic direction, while individual stakeholders shall be accountable for specific aspects of implementation. No AI system shall be deployed without the explicit approval of the AIGC, and all deployments shall be subject to continuous monitoring and periodic review using the **Impact Assessment Tool** set out in **Appendix B**.

3.2 The AI Governance Framework

3.2.1 The AI Governance Committee (AIGC)

The Integrated Case Management Systems (ICMS) Committee shall serve as the AI Governance Committee (AIGC). The AIGC is responsible for providing strategic direction, oversight, and accountability. The Committee shall:

a) Approve AI-related projects, frameworks, and policies to ensure alignment with the Judiciary's mandate and applicable legal frameworks.
b) Monitor compliance with data protection requirements, ethical standards, and fairness principles across all AI systems deployed within the Judiciary.
c) Advise the Chief Justice on emerging AI risks, opportunities, and technological developments to support informed decision-making and responsible innovation.

3.2.2 Roles and Responsibilities

The successful implementation of this Policy requires a clear delineation of roles, as outlined below:

a) **Chief Justice / Judicial Service Commission (JSC):** Provide strategic oversight, policy approval, and accountability; ensure AI adoption aligns with constitutional values.

b) **AI Governance Committee (AIGC):** Evaluate, approve, and monitor AI systems; set compliance standards; advise the Chief Justice on emerging risks.

c) **Judges and Judicial Officers:** Ensure responsible use of AI, maintain human oversight, interpret AI outputs cautiously, and exercise independent judgment.

d) **ICT Directorate:** Provide technical validation, cybersecurity assurance, vendor assessment, and ensure systems are secure and compliant.

e) **Kenya Judiciary Academy (KJA):** Build capacity, provide ethics training, and ensure AI literacy for all judicial officers and staff.

f) **Third-party vendors and technology partners:** Comply with all contractual, ethical, and regulatory requirements; ensure privacy-by-design; submit to independent audits; and guarantee data security. No AI solution shall be procured or deployed without prior approval by the AIGC.

Chapter 4: Artificial Intelligence Systems Risk Management Framework

The integration of Artificial Intelligence into the judicial system presents significant opportunities to enhance efficiency, improve access to justice, and strengthen the quality of legal processes. However, the deployment of such technologies, particularly within a constitutional democracy, also introduces risks that should be carefully and responsibly managed.

This chapter establishes the framework for the identification, assessment, and mitigation of risks associated with the development, procurement, deployment, and use of AI systems within the Judiciary. The framework is designed to uphold constitutional guarantees, safeguard judicial independence, and maintain public trust in the administration of justice. It adopts a continuous, lifecycle approach to risk management, ensuring that AI tools are subject to rigorous oversight from initial conception through deployment, monitoring, and eventual decommissioning.

The provisions in this chapter provide guidance on the responsible use of AI within the Judiciary and require that all AI applications adhere to the highest ethical standards and constitutional principles, including fairness, privacy, equality, and access to justice. They promote a culture of proactive risk management, ensuring that technological innovation supports and strengthens the integrity of the judicial process.

This framework applies to all AI systems and tools, regardless of their perceived complexity or function, that are:

a) Developed in-house by the Judiciary's ICT directorate or any of its agencies,
b) Procured or licensed from third-party vendors and external suppliers, or
c) Deployed for use by judicial officers, court administrators, and support staff in the execution of their official duties.

The policy guidance below covers the entire lifecycle of an AI system, including its planning, development or procurement, piloting, deployment, and continuous monitoring.

4.1 Policy Direction on Risk Management

It is the policy of the Judiciary that all AI systems shall be governed by a principle-based risk management framework. The cornerstone of this policy is the classification of AI systems by risk level, which determines the stringency of oversight, validation, and control measures required. All AI initiatives shall undergo a continuous and iterative risk assessment process that integrates legal, ethical, technical, and operational perspectives. The Judiciary shall adopt a precautionary approach: where potential risks are intolerable

or cannot be effectively mitigated, the deployment of the AI system shall be prohibited. For all other risks, a hierarchy of controls, including human oversight, transparency, and independent audit, shall be applied.

4.2 The AI Risk Management Framework

To operationalize this policy, all AI systems deployed within the Judiciary shall undergo a continuous risk assessment throughout their lifecycle, structured across the following four key stages:

a) **Planning Stage: Fundamental Rights and Ethical Impact Assessment**

Prior to the approval or procurement of any AI initiative, a mandatory Judicial AI Impact Assessment (JAIIA) shall be conducted as set out under **Appendix B**. This assessment shall evaluate the proposed system's potential impact on core constitutional rights, including but not limited to the right to privacy, equality before the law, access to justice, and a fair hearing. It shall analyse the intended functionality, data sources, potential for bias, and proportionality of the technology to its stated legal and administrative purpose. The findings, including proposed safeguards and an analysis of impacts on vulnerable groups, shall inform the project's design, populate the initial risk register, and be submitted to the AI Governance Committee for review prior to project approval.

b) **Development and Procurement Stage: Risk Classification and Quality Audits**

At this stage, each AI system shall be formally classified according to its risk level, as detailed in **Appendix C: AI Risk Classification Matrix**. This classification dictates the necessary level of due diligence, validation, and contractual oversight. Concurrently, comprehensive bias and data quality audits shall be conducted to verify that training data is accurate, representative, and free from discriminatory patterns.

All procurement contracts with vendors shall explicitly include clauses pertaining to data provenance, rigorous testing obligations, and full audit access rights to ensure ongoing transparency and accountability.

c) **Deployment Stage: Controlled Pilots and Human Oversight**

Before full-scale implementation, all AI systems, particularly those classified as medium- or high-risk, shall undergo controlled piloting in designated court environments. These pilots are to assess functionality, accuracy, usability, and integration with existing systems like the Integrated Case Management System (ICMS).

During deployment, robust cybersecurity safeguards, including encryption, network segmentation, and strict authentication controls, are mandatory. Critically, all deployed

systems shall incorporate human oversight mechanisms to ensure that final judicial or administrative decisions remain under the exclusive control of qualified officers.

AI outputs shall be explainable and auditable, empowering judicial officers to understand, question, or override any algorithmic suggestions.

d) **Monitoring Stage: Continuous Evaluation and Risk Register Maintenance**

Post-deployment, every AI system is subject to continuous monitoring and periodic review to ensure sustained compliance with performance, fairness, and evolving legal standards. The Judiciary shall maintain a dynamic and up-to-date AI Risk Register, documenting all identified risks, incidents, mitigation measures, and responsible officers. Ongoing evaluation activities shall include real-time performance analytics, bias re-testing, and system audits to detect algorithmic drift or unintended consequences. All incidents, from system errors to ethical breaches, shall be formally logged, investigated, and documented. These findings shall be reported regularly to the AI Governance Committee to inform policy updates and ensure the framework remains responsive and effective, thereby reinforcing public trust in the Judiciary.

A detailed **Risk Matrix** is provided in **Appendix C: AI Risk Matrix**, outlining primary risk categories, their descriptions, severity levels, required actions, and key controls.

Chapter 5: Management of AI Tools and Third-Party Systems

The Judiciary may rely on a combination of internally developed and commercially procured AI tools to support its operations. This chapter establishes the standards for the selection, procurement, vetting, and management of all AI systems used within the Judiciary, with particular emphasis on due diligence for third-party vendors and the responsible use of publicly available generative AI tools. These measures are essential to safeguard judicial data, preserve system integrity, and maintain public trust.

The framework set out in this chapter ensures that the development, procurement, and use of AI tools are conducted in a secure, ethical, and accountable manner. It requires that all external engagements adhere to the highest standards of integrity and compliance, and that the use of third-party AI systems does not compromise judicial independence, data protection obligations, or the confidentiality of judicial information.

5.1 Policy Direction on AI Tools and Vendors

It is the policy of the Judiciary that all third-party engagements shall adhere to strict standards of integrity and accountability. Vendors shall be held to the highest ethical and operational benchmarks. Furthermore, the use of all third-party AI tools, especially generative systems, shall be governed by clear rules to protect sensitive information.

The Judiciary prohibits the use of any external AI tool for processing confidential case-related information.

5.2 The Framework for AI Tool Management

5.2.1 AI Tool Selection and Third-Party Due Diligence

The Judiciary shall ensure that all third-party engagements in the design, supply, or maintenance of AI systems adhere to clear standards of integrity, accountability, and legal compliance. Given the sensitivity of judicial data and the constitutional imperative to preserve judicial independence, external vendors and technology partners shall be subject to rigorous due diligence and oversight. The requirements outlined below establish the minimum standards for vendor assessment, contractual safeguards, data governance, certification, and technical validation to ensure that all AI systems procured or deployed within the Judiciary are secure, trustworthy, and aligned with applicable legal and ethical obligations. The minimum procurement and partnership requirements are set out in **Appendix D: AI Tool Selection and Third-Party Due Diligence Requirements**.

5.2.2 Use of Third-Party AI Tools and Generative Systems

The Judiciary acknowledges the increasing availability and use of publicly accessible artificial intelligence tools. This section sets out standards to ensure their responsible, lawful, and secure use within the Judiciary.

a) **Permitted scope of use:** Third-party AI tools may only be used for administrative, research, or drafting support functions that do not involve the processing of confidential, privileged, or personally identifiable judicial data. Permitted uses include generating meeting agendas, drafting internal memoranda, or using grammar and style tools to edit public-facing documents.

b) **Prohibited activities:** Third-party AI tools shall not be used to process, summarise, or generate outputs based on case files, evidence, witness statements, judgments yet to be delivered, or internal judicial deliberations. The uploading of pleadings or other case-related materials, the use of AI to draft judgments, or requesting AI systems to interpret or predict outcomes in ongoing proceedings is strictly prohibited.

c) **Verification and accountability:** Any AI-generated content shall be treated solely as informational and shall be independently verified by a human user. Judicial officers and staff shall review and confirm the accuracy, context, and reliability of all AI outputs before relying on them for official use.

d) **Citing legal sources:** Officers shall ensure that all legal references are drawn from original and verifiable sources, such as statutes, judicial precedents, or official law reports, and shall not rely on AI-generated text as a primary legal authority.

e) **Data protection and confidentiality:** Confidential or restricted information shall not be uploaded, pasted, or otherwise disclosed to third-party AI systems. The use of external AI platforms shall comply fully with the Data Protection Act and all applicable internal confidentiality and data governance requirements of the Judiciary.

A detailed checklist for compliance is provided in **Appendix E: Checklist for Use of Third-Party AI Tools and Generative Systems**.

Chapter 6: Capacity Building and AI Literacy

The responsible use of Artificial Intelligence depends on the knowledge, skills, and judgment of the individuals who interact with it. This chapter outlines the Judiciary's commitment to strengthening institutional capacity by ensuring that judicial officers and staff are equipped with the competencies required to understand, supervise, and responsibly use AI tools in the course of their duties.

This chapter establishes a structured capacity-building and AI literacy framework aimed at enabling Judiciary personnel to use AI effectively while remaining alert to its ethical, legal, and operational risks. The objective is to ensure that technological tools enhance productivity and efficiency while preserving human judgment, professional responsibility, and ethical standards.

This framework applies to all Judiciary personnel, including judges, magistrates, Kadhis, tribunal members, registrars, researchers, ICT personnel, and administrative staff.

6.1 Policy Direction on Capacity Building

It is the policy of the Judiciary that continuous education on AI is mandatory for all personnel. The Kenya Judiciary Academy (KJA) shall integrate AI ethics and governance into its core curricula. Training shall be practical, role-specific, and ongoing to keep pace with technological advancements.

6.2 The AI Literacy Framework

a) **Integration into Judicial Training:** The KJA shall integrate AI Ethics and Governance into its curricula, including modules on fairness, transparency, and accountability in AI-assisted decision-making.

b) **Regular Workshops:** Regular workshops shall be organized for judges, registrars, and ICT teams on key topics such as data protection, automation bias, and algorithmic accountability.

c) **Collaborations:** The Judiciary shall collaborate with universities and international partners to align training content with global best practices.

d) **Mandatory Orientation:** All judicial officers and staff shall undergo mandatory orientation on the responsible use of generative AI tools, covering all related risks.

e) **Short Course and Internal Guidelines:** KJA shall design a short course and issue internal guidelines on the appropriate use of AI in research, writing, and administrative support.

f) **Continuous Awareness:** The Judiciary shall conduct periodic awareness campaigns and reminders emphasizing that confidentiality obligations and institutional reputation take precedence over convenience.

Chapter 7: Implementation, Practice Directions, and Continuous Review

This chapter translates the objectives of this Policy into a clear and actionable implementation framework. It outlines the phased approach for the adoption and operationalisation of AI within the Judiciary, the process for developing binding Practice Directions, and the mechanisms for monitoring and continuous improvement to ensure the Policy remains responsive to evolving technologies.

It provides a roadmap for the effective and consistent application of the Policy across the Judiciary and establishes procedures for the development of detailed rules, Standard Operating Procedures (SOPs), and Practice Directions governing the use of AI. This chapter applies to all implementation activities arising from this Policy and supports a continuous review cycle to ensure that AI governance remains current, responsible, and aligned with the Judiciary's legal and constitutional obligations.

7.1 Policy Direction on Implementation and Review

It is the policy of the Judiciary that the implementation of this Policy shall be phased, evidence-driven, and subject to rigorous monitoring and evaluation. Furthermore, recognizing the dynamic nature of AI, this Policy shall be a living document, subject to regular review and updates to address emerging challenges and opportunities.

7.2 The Implementation and Practice Framework

7.2.1 Phased Implementation Approach

Effective implementation requires a coordinated and sequenced approach. The workflow below outlines the key steps the Judiciary shall take to plan, operationalize, and monitor the responsible use of AI. A detailed **Implementation Matrix** with specific activities, deliverables, KPIs, and timelines is provided in **Appendix F: AI Policy Implementation Matrix**.

Step 1: Institutional governance and human capacity development
The first phase focuses on establishing the people and structures that will guide AI integration. The Judiciary shall constitute an AI Governance Committee (AIGC)to provide high-level governance, policy alignment, and oversight of all AI-related activities. This committee will ensure that AI initiatives uphold constitutional values, judicial independence, and the principles of fairness, privacy, and accountability.

Once governance structures are in place, a structured capacity-building programme shall be rolled out. Judges, magistrates, registrars, researchers, and ICT personnel shall be

trained on AI ethics, data privacy, bias detection, and responsible interpretation of algorithmic outputs.

Step 2: Embedding risk-based processes and accountability mechanisms
The second phase operationalizes internal controls to manage risks associated with AI. The Judiciary shall adopt a risk management framework for AI systems that identifies and documents potential legal, ethical, and operational threats across the AI lifecycle from design and procurement to deployment and retirement. Each AI initiative shall maintain a risk register outlining vulnerabilities, controls, and mitigation measures.

Step 3: Developing secure and interoperable technology infrastructure
Once governance and processes are established, the focus shifts to building a robust technological foundation. The Judiciary shall design an AI-ready architecture that is secure, scalable, and interoperable across divisions and court stations. This infrastructure shall support integration with existing systems such as the ICMS and e-filing platform while safeguarding data integrity and confidentiality.

Step 4: Phased adoption and piloting of AI use cases
The Judiciary shall adopt a phased and evidence-driven approach to introducing AI applications. Initial pilots shall focus on high-backlog or document-intensive areas, such as transcription, legal research assistance, or case allocation. These early deployments shall be designed to test functionality, assess user experience, and evaluate efficiency gains. A pilot–evaluation scale cycle shall guide implementation.

Step 5: Monitoring, evaluation, and continuous improvement
The final phase institutionalizes learning and accountability. The Judiciary shall establish a Monitoring, Evaluation and Learning (MEL) Framework for AI implementation, anchored within the ICMS Committee and supported by the Judiciary Performance Management Directorate.

7.2.2 Development of Practice Directions for AI Use in Courts and Tribunals

To ensure uniformity and ethical integrity, specific Practice Directions shall be developed to guide the use of AI tools within court and tribunal proceedings. The development of these Practice Directions shall be participatory and transparent, involving judges, magistrates, tribunal members, ICT experts, the Law Society of Kenya (LSK), Court User Committees (CUCs), and relevant oversight institutions to ensure practical applicability.

7.3 Continuous Review

Given the evolving nature of generative AI, this Policy shall remain adaptive. The Judiciary, through the AI Governance Committee, shall continuously monitor emerging technologies

like large language models, automated transcription, and AI-powered summarization. The Policy, along with its associated Practice Directions and SOPs, shall be formally reviewed and updated at least annually, or more frequently as needed, to ensure the safe, ethical, and transparent use of such tools within judicial processes.

Appendices

Appendix A: AI Guiding Principles Framework

Principle	Policy Statement	Key Considerations
Legality and Trustworthiness	AI systems should be lawful, secure, and anchored in the Constitution and relevant laws.	Judicial oversight Data protection compliance Human review of AI recommendations.
Inclusivity and Accessibility	AI tools should be people-centred and inclusive, particularly for marginalized groups.	Local language interfaces Disability access Support for areas with limited infrastructure.
Fairness and Bias Prevention	The Judiciary shall prevent algorithmic bias and ensure no group is discriminated against.	Routine bias audits Representative datasets Complaint mechanisms.
Transparency and Explainability	AI use should be disclosed, and systems should explain their outputs in plain language.	Public notices Model explainability Audit trails.
Human Oversight and Accountability	Judicial officers retain authority over all AI recommendations.	Governance bodies Clear oversight mechanisms Ethical accountability.
Security and Reliability	AI systems should protect against cyber threats in line with the Computer Misuse and Cybercrimes Act (2018).	Threat detection Regular testing System resilience.

Principle	Policy Statement	Key Considerations
Judicial Independence	AI should not undermine judicial autonomy under Article 160.	No external control Data sovereignty Transparent procurement.
Efficiency and Sustainability	AI should enhance case management and resource allocation while safeguarding fairness.	Performance tracking Balance between speed and fairness Adaptive learning systems.
Local led	AI tools utilised should reflect the communities that the Judiciary serves therefore need to be locally led innovations or tested locally.	Culturally sensitive and relevant Data should be stored locally.

Appendix B: Judicial AI Impact Assessment (JAIIA) template

1. Project Overview	
Item	**Details / Input**
1.1 Name of AI System / Tool	
1.2 Purpose and Intended Use	
1.3 Problem the AI Tool Seeks to Solve	
1.4 Court / Tribunal / Department	
1.5 Project Lead (Name, Role, Contact)	
1.6 Vendor / Developer Information	
1.7 Stage of Deployment	Prototype / Pilot / Testing / Deployment / Review
2. Description of the AI System	
Item	**Details / Input**
2.1 Type of AI System	GenAI / NLP / Predictive / Automation / Other
2.2 Key Functionalities	
2.3 Inputs Required	
2.4 Outputs Produced	
2.5 Technical Architecture (Cloud/On premises)	
2.6 Integration Points (CMS, e-filing, etc.)	
2.7 Data Storage and Retention	
3. Legal and Ethical Basis	
Item	**Details / Input**
3.1 Constitutional Alignment	Articles 10, 27, 28, 31, 47, 48, 50, 159
3.2 Statutory Alignment	KDPA, Fair Administrative Action, Evidence Act, Judicial Code
3.3 Legal Basis for Processing Data	Judicial function / Public interest / Legal obligation

3.4 Compatibility with Judicial Independence	Impact assessment notes			
3.5 Ethical and Professional Standards	Risks to fairness, impartiality, neutrality			
4. Data Description and Governance				
Item	**Details / Input**			
4.1 Categories of Data Used	Case files, judgments, witness statements, etc.			
4.2 Sensitivity of Data	Personal / Special category / Privileged / Confidential			
4.3 Data Sources	Internal / External / Third-party			
4.4 Data Flows Diagram Summary				
4.5 Anonymisation / Pseudonymisation Measures				
4.6 Data Minimisation Steps				
4.7 Data Storage Location				
4.8 Data Security Controls	Encryption, access logs, and authentication			
4.9 Retention and Deletion Plan				
5. Risk Identification and Analysis				
Risk Category	**Description of Risk**	**Likelihood**	**Impact**	**Risk Level**
Judicial Risks	Automation bias, undue influence, fairness			
Data Protection Risks	Breach, unlawful processing, over-collection			
Ethical Risks	Bias, discrimination, unfair outcomes			
Operational Risks	System failure, inaccurate outputs, downtime			

Cybersecurity Risks	Attacks, adversarial manipulation, model theft			
Access to Justice Risks	Digital divide, unequal access to tools			
Reputational Risks	Public trust erosion, perceived bias			
6. Risk Mitigation Plan				
Identified Risk	**Mitigation Strategy**	**Responsible Person**	**Timeline**	**Residual Risk**
7. Human Oversight and Accountability				
Item	**Details / Input**			
7.1 Human Oversight Model	Human-in-the-loop / Human-on-the-loop / Human-out-of-the-loop			
7.2 Roles and Responsibilities	Judges, registrars, ICT officers, DPO			
7.3 Decision Override Mechanisms				
7.4 Error Escalation Pathways				
7.5 Accountability Assignments	(e.g., Project Owner, DPO, ICT Lead)			
8. Transparency and Explainability				
Item	**Details / Input**			
8.1 Explainability Measures	Model cards, documentation, logs			
8.2 User Guidance Documentation				
8.3 Transparency to Litigants	Notice provided? Procedure?			
8.4 Public Disclosure Requirements	Courts rules/practice directions			
8.5 Audit Trails and Logs				
9. Procurement and Vendor Risk Management				
Item	**Details / Input**			
9.1 Vendor Due Diligence Completed	Yes/No			
9.2 Security Certifications				
9.3 Contractual Safeguards	DPAs, NDAs, SLA terms			

9.4 Prohibition on Secondary Use of Judicial Data	Yes/No
9.5 Data Processing Agreement Signed	Yes/No
9.6 Exit and Transition Plan	
10. Testing, Validation and Quality Assurance	
Item	**Details / Input**
10.1 Testing Approach	Accuracy, stress tests, bias testing
10.2 Test Datasets Used	
10.3 Accuracy and Performance Metrics	
10.4 Bias Assessment Findings	
10.5 User Acceptance Testing Results	Feedback from judges/magistrates/researchers/registrars
10.6 Security Testing Results	
11. Public Participation and Stakeholder Engagement	
Item	**Details / Input**
11.1 Stakeholders Consulted	Judiciary, LSK, academia, civil society, ODPC, CA, NC4, MOICDE
11.2 Summary of Feedback	
11.3 Issues Raised	
11.4 Changes Made to System Based on Feedback	
11.5 Additional Engagement Required	
12. Monitoring, Evaluation and Continuous Review	
Item	**Details / Input**
12.1 Key Performance Indicators	Speed, accuracy, fairness, user satisfaction
12.2 Monitoring Plan	Monthly / Quarterly / Annually
12.3 Incident Reporting Procedure	
12.4 Continuous Improvement Plan	
12.5 Decommissioning Conditions	
13. Final Recommendation and Approval	
Item	**Details / Input**
13.1 Summary Conclusion	

13.2 Conditions for Approval			
13.3 Approvers Required	CJ / ICT Directorate / DPO / Registry Lead		
Sign-off			
Name	**Position**	**Signature**	**Date**

Appendix C: AI Risk Classification Matrix

Category	Description	Risk Level	Recommended Action & Oversight
Judicial Decision-Support AI	Tools aiding legal interpretation, evidence review, or outcome prediction.	**High-Risk**	**Mandatory Human Oversight:** All outputs shall be verified. **Prohibit Reliance:** AI shall not substitute judicial reasoning. **Mandatory Approvals:** Require formal authorization by JSC/Chief Registrar, bias audits, and transparent documentation.
Administrative / Support AI	Tools for scheduling, document management, anonymization.	**Medium-Risk**	**Role-Appropriate Deployment:** Limit to administrative functions. **Periodic Validation:** Supervisors to review accuracy quarterly. **Access Controls:** Restrict user permissions.
Non-Critical AI	Analytics, communication bots, workflow automation.	**Low-Risk**	**Encourage Innovation:** Staff may use with basic caution. **Monitor Output:** Review outputs before sharing. **Prevent Data Leaks:** Avoid inputting identifiable information.

Appendix C: AI Risk Matrix

Risk Category	Description	Risk Level	Required Action	Key Controls
Bias and Discrimination	Algorithmic unfairness disadvantaging protected groups.	High	Mitigate	Bias audits Fairness metrics Redress mechanisms
Transparency / Explainability	Inability to understand AI logic.	High	Mitigate	Documentation User disclosure Audit trails
Automation Bias	Over-reliance on AI outputs, undermining judicial independence.	Intolerable	Avoid	Human oversight Override rights Judicial training
Rights Infringement	Breach of fair trial, privacy, or judicial independence.	Intolerable	Prohibit	FRIA/JAIIA Judicial redress pathways
Data Quality and Security	Poor data or cyber breaches.	Moderate	Manage	Data governance Encryption Access controls
System Robustness	Technical errors or instability.	Moderate	Manage	Testing Redundancy Continuous monitoring

Appendix D: AI Tool Selection and Third-Party Due Diligence Requirements

Area	Requirements
Vendor Assessment	Evaluate vendor integrity, independence, and compliance with judicial ethics.
Contractual Clauses	Define accountability, audit rights, and Service Level Agreements (SLAs).
Data Transfers	Cross-border data processing should comply with KDPA and include adequate safeguards.
Certification and Trust	Prefer certified AI systems (ISO/IEC 42001 or equivalent) and vendors with transparent governance.
Testing and Validation	Require pre-deployment validation, red-teaming, and adversarial testing.

Appendix E: Checklist for Use of Third-Party AI Tools and Generative Systems

Compliance Item	Requirement / Standard	Allowed?	Verification / Evidence Required
Purpose of AI Use	AI tools are used only for administrative, research, or drafting support roles.	✓ Allowed	Officer confirms task is non-sensitive.
Non-Sensitive Data Only	No confidential, privileged, or personally identifiable judicial data is used.	✓ Allowed	Review of inputs before submission.
Case-Related Data	AI tools shall not be fed any case files, pleadings, evidence, or bench notes.	✗ Prohibited	Random checks Officer self-declaration.
Drafting of Judgments	AI cannot draft, assist, summarize, or edit judgments or judicial deliberations.	✗ Prohibited	Audit trail of drafting process.
Processing of Case Management Info	AI tools cannot analyse, interpret, or summarize case management data.	✗ Prohibited	System access logs checked.
Verification of AI Outputs	All AI outputs shall be independently reviewed, validated, and edited by the officer.	✓ Mandatory	Evidence of fact-checking (cross-referencing).
Original Legal Sources Used	Officers cite original statutes, case law, and official records, not AI-generated text.	✓ Mandatory	Official citations included in drafts.
Data Protection Compliance	Use shall comply with KDPA, Judicial Service Act, and internal confidentiality policies.	✓ Mandatory	Compliance checklist signed.
Use of Dummy Data in Training	Staff training shall use dummy or hypothetical data.	✓ Required	Training materials reviewed.

Compliance Item	Requirement / Standard	Allowed?	Verification / Evidence Required
Misuse Reporting Mechanism	Officers may report misuse/confidentiality breaches through internal channels.	✓ Mandatory	Report logged in HR or ICT systems.