

BAYELSA MEDICAL UNIVERSITY

YENAGOA, BAYELSA STATE



Artificial Intelligence Policy and Governance

Policy owner: Bayelsa Medical University

1 October 2026

Preface

Artificial intelligence is increasingly used in university education, research and administration. Its benefits depend on informed use, careful verification and

clear accountability. Bayelsa Medical University's Artificial Intelligence Policy and Governance provides a common framework for staff and students to use these technologies responsibly while protecting academic integrity, confidentiality, fairness and patient safety.

The policy establishes requirements for AI disclosure, assessment, research, institutional approval and oversight. It recognises that AI may support learning and professional work, while responsibility for the accuracy, integrity and consequences of that work remains with the people undertaking it.

From 1 October 2026, staff and students who use AI in their studies, teaching, assessment or research shall declare that use, identify the software or tool and explain how it was used.

The University AI Committee coordinates implementation. Functions requiring specialist expertise, statutory authority or independence remain with the appropriate officers and bodies. This arrangement provides clear responsibility while preserving professional standards and established University procedures.

All staff and students are expected to understand and apply the provisions relevant to their activities. Through continuing education, monitoring and periodic review, the University will support responsible innovation and maintain confidence in its academic and professional work.

Prof. Dimie Ogoina

Vice Chancellor

Acknowledgements

Bayelsa Medical University gratefully acknowledges the members of the University AI Committee for their contributions to the development of this Artificial Intelligence Policy and Governance document.

Special appreciation is extended to Prof. Chidinma Daokoru-Olukole, Dr. Sylvester Izah and Dr. Julius Wosowei for their valuable contributions to this work. Their involvement is sincerely appreciated, alongside the collective efforts of other committee members.

The University also recognises the importance of cooperation across its academic and administrative units in implementing this policy. The participation of staff and students will be essential to promoting transparent AI use, protecting academic integrity and ensuring that technological innovation supports the University's educational, research and service responsibilities.

DRAFT DOCUMENT

Contents

- 1 Purpose scope and commencement
- 2 Responsibility and governance
- 3 AI declaration and evidence requirements
- 4 Permitted use and prohibited conduct
- 5 Teaching assessment and academic integrity
- 6 Research publication and intellectual property 7 Risk assessment and approval
- 8 Privacy security and information management
- 9 Clinical administrative and public use
- 10 Inclusion training and continuity
- 11 Incidents complaints and corrective action
- 12 Implementation monitoring and review

1 Purpose scope and commencement

1.1 Purpose and coverage

This policy governs the responsible use, development, procurement and oversight of artificial intelligence at Bayelsa Medical University (BMU). It protects academic integrity, patient safety, confidentiality, fairness and accountable human judgement while permitting appropriate innovation.

The policy applies equally to all academic and non-academic staff and all undergraduate and postgraduate students. It also applies to adjunct and temporary staff, visiting researchers, interns, consultants and contractors undertaking University work. It covers teaching, private study related to University programmes, assessment, research, publication, clinical placements, administration and public communication, whether on campus, remotely or during fieldwork.

AI includes generative text, images, audio, video and code; predictive and classification systems; automated recommendations; AI embedded in ordinary software; and agents that perform actions. Free tools, paid subscriptions, personal accounts and locally developed systems are within scope when used for University activities.

1.2 Commencement and mandatory declaration

From 1 October 2026, every staff member and student who uses AI in their studies, teaching, assessment, research or scholarly output shall declare that use, identify the software or tool, and explain how it was used. Section 3 specifies the information, placement and records required. The requirement applies to work submitted, resubmitted, presented or published from that date, including ongoing work containing earlier AI assistance.

1.3 Authority and interpretation

Applicable Nigerian law, binding professional obligations and the University's statutes take precedence. This policy supplements existing academic, employment, research, clinical, procurement and information-security rules. Clinical activities remain subject to the authorisation of the responsible institution.

Bayelsa Medical University owns this policy. The University AI Committee coordinates its implementation and provides guidance on interpretation, with legal or specialist advice where required. The Vice Chancellor shall retain formal institutional approval records and resolve procedural questions within the University's established authority.

2 Responsibility and governance

2.1 University AI Committee

The University AI Committee shall coordinate implementation, publish guidance and reporting routes, maintain the approved-tool and deployment registers, organise staff and student training, monitor declarations, arrange risk reviews, track corrective action and prepare quarterly implementation reports. The committee is responsible for routine policy administration, disclosure guidance, awareness, monitoring and policy review.

Each department shall nominate a contact to assist the University AI Committee. Delegation shall be recorded by role, task, scope and duration. A project's operational owner remains responsible for its outputs and controls; central coordination does not transfer the professional duties of lecturers, researchers or clinicians.

2.2 Specialist responsibilities

The following functions require specialist competence, statutory authority or independence. Where the relevant position is vacant, the Vice Chancellor shall appoint or formally designate a suitably qualified officer, or arrange access to an authorised external body. Until then, an activity requiring that function shall not proceed. Designation shall preserve applicable independence requirements.

Director of Academic Planning: advise on lawful processing, privacy impact assessments, data-subject rights, international transfers and personal-data breaches; maintain the regulatory compliance schedule. The University AI Committee shall not override independent privacy advice.

Head of ICT: lead security assessment, access control, integrations, technical incident containment, backups and system restoration. The Head of Estates shall support assessment of physical hazards and protection of equipment.

Head of Department and Course Coordinator: approve assessment instructions within academic authority, ensure declarations accompany submissions, arrange moderation and support students. The supervisor and Principal Investigator shall oversee research methods, evidence and project-specific compliance.

The Clinical Safety Lead, appointed by the responsible clinical institution, shall oversee patient-facing validation, professional supervision and clinical incidents.

The Legal Adviser shall advise on legal interpretation, contracts and required notifications.

Head of Procurement and Bursar: conduct acquisition, contract and financial controls within their respective authority. The Head of Communications shall authorise public institutional messaging through established sign-off arrangements.

Head of Internal Audit: provide independent assurance. The University AI Committee and operational owners shall not independently audit or adjudicate their own actions. A conflict involving the University AI Committee shall be referred to the Registrar for an independent reviewer.

2.3 Oversight and decisions

The Vice Chancellor shall ensure resources, specialist appointments and escalation to Senate or Governing Council within their respective powers. The University AI Committee shall convene academic, technical, privacy, legal and clinical reviewers as relevant, with staff and student representation for policy-wide matters. This arrangement shall respect existing institutional authority.

Decisions shall record the evidence considered, conflicts of interest, reasons, conditions, responsible officers and review dates. Conflicted reviewers shall withdraw from the decision. High-risk approval requires the competent institutional authority and relevant specialist clearances; the University AI Committee coordinates the process and records the outcome.

3 AI declaration and evidence requirements

3.1 What must be declared

Staff and students shall declare AI assistance used for ideas, literature discovery, summaries, translation, language editing, drafting, rewriting, coding, statistical analysis, data extraction, screening, images, presentations or other study and research tasks. AI-enabled editing is included even when described as grammar support. Ordinary non-AI spelling checks, calculators and reference-management functions do not require an AI declaration unless the task instructions require reporting them.

The declaration shall identify the tool or software name, provider, model or version where available, and date or period of use. It shall describe the task performed, the parts of the work affected, the extent of the assistance, and the human checks or corrections made. If the version is unavailable, state “version not displayed”; do not invent a version. Declare each tool when more than one was used.

3.2 Where and when to declare

Students shall place an AI Use Declaration in each relevant assignment, project, dissertation, thesis, practical report or presentation. Staff shall include it in relevant teaching materials, research reports, manuscripts, grant applications and scholarly presentations. For publications, also comply with the journal’s required manuscript section and submission disclosure. AI used in research methods shall be described sufficiently in the methods section for scrutiny and reproducibility.

A concise declaration within the work is sufficient. For assessed or research submissions in which no AI was used, include the no-use statement. For group work, disclose the tools used by all contributing members and identify the affected contributions.

3.3 Examples and records

Declaration example: “I used [tool and provider; version if available] during [period] to [specific tasks] in [sections or outputs]. I checked [sources, calculations, code or other evidence] and made [relevant corrections]. I take

responsibility for the final work.” Complete only the checks actually performed.

No-use statement: “I did not use AI tools in preparing this work.” For joint work, use “We” and obtain confirmation from all contributors.

Keep relevant drafts, source notes, analysis code and necessary prompt/output extracts in approved storage for the period required by the assessment, research or records schedule. Do not retain unnecessary personal data or upload confidential material merely to document AI use. Staff and students shall not be required to surrender passwords or unrelated personal account content.

3.4 Errors and omissions

A person discovering an omitted or inaccurate declaration shall promptly notify the recipient and submit a dated correction. For research already submitted or published, the responsible author shall follow the journal’s or sponsor’s correction procedure.

The University AI Committee shall monitor declaration compliance through proportionate sampling and departmental reports. Course staff and research supervisors shall check that declarations are present at receipt; they remain responsible for evaluating the underlying work. AI disclosure is an academic transparency requirement, not a declaration that every AI-assisted activity is acceptable.

4 Permitted use and prohibited conduct

4.1 Conditions of responsible use

Every institutional AI use must have a named owner, a stated purpose and an explanation of why it is appropriate. A person who uses an output in teaching, research, administration or clinical work remains responsible for checking it within their competence. Responsibility cannot be transferred to a vendor disclaimer or an AI-generated assurance. Where a user lacks the expertise to verify a consequential output, they must obtain competent review or avoid using it. Human review must be substantive and capable of changing the outcome.

Staff and students may use approved tools for authorised learning, drafting, analysis and administrative assistance. They shall check factual claims, sources, calculations, code and relevant limitations before reliance. A paid subscription, public availability or declaration alone does not establish approval for a particular purpose or data category.

4.2 Prohibitions

Staff and students shall not use AI to fabricate data, research participants, experiments, clinical encounters, references, signatures, qualifications, attendance or assessment evidence; impersonate another person; conceal unauthorised assistance; or produce deceptive University announcements. AI shall not be used to evade examination rules, bypass access controls, harass people or create non-consensual deceptive representations of a person's image or voice.

Confidential information shall not be entered into an unapproved service. AI shall not perform generalised social scoring or infer honesty, suitability or emotion from appearance or voice for consequential institutional decisions. Synthetic examples shall be labelled and shall not be represented as observations.

BMU prohibits AI-only final decisions on grades, admissions, scholarships, academic progression, recruitment, promotion and patient management. A competent human decision-maker must review the evidence and retain authority to change the outcome. A signature without substantive review does not meet this requirement.

4.3 Rights and review

People affected by significant AI-supported decisions shall receive an understandable account of AI's role and a route to human review, correction or appeal, subject to lawful limits. Good-faith reporting and questioning of outputs shall not attract retaliation. Human-centred education and health governance inform these safeguards (Miao & Holmes, 2023; World Health Organisation, 2021).

5 Teaching assessment and academic integrity

5.1 Teaching and independent competence

Lecturers shall verify AI-assisted teaching materials before distribution, disclose assistance under Section 3, and preserve the knowledge and reasoning students must develop independently. Generated cases must be identified as synthetic. AI output cannot substitute for a laboratory procedure, clinical examination or practical skill that was not performed.

Students may use approved tools for permitted explanations, practice and comparison of approaches, but shall verify important responses against course materials and reliable sources. Students must be able to explain the reasoning, sources and methods in their submitted work.

5.2 Assessment permissions

Every assessment brief shall identify one permission level: independent work, with no AI-generated assessed content; limited assistance for specified tasks; integrated AI use within stated boundaries; or AI-focused assessment of the use and critique of AI. The brief shall state the permitted and prohibited activities, declaration and evidence requirements, and any accessible alternative.

The Course Coordinator shall issue the instruction before work begins and obtain departmental approval where required. If instructions are unclear, students shall seek clarification before generating assessed content. Approved accessibility support remains governed by its specific authorisation. New restrictions shall not be applied retrospectively to work completed under materially different instructions.

Examinations shall specify permitted devices and AI-enabled functions. Process evidence may include drafts, source notes, practical demonstrations and proportionate oral explanation. Such requirements shall be communicated in advance and shall accommodate disability and documented disruption.

5.3 Marking and verification

AI may assist marking or feedback only within an approved, validated and privacy-protected process. The assessor remains responsible for each consequential result; final grades remain subject to ordinary moderation and approval. Staff shall not upload student work or examination materials to unapproved services.

An AI detector score, writing style or change in language shall not be treated as conclusive evidence of how work was produced. Staff shall use source verification, relevant drafts and discussion with the author to clarify concerns. Reviews shall remain confidential and give staff and students an opportunity to explain their work.

5.4 Fair access

No compulsory learning activity shall require a personal paid subscription unless the University provides equitable approved access or an equivalent route without disadvantage. A non-AI route must assess the same intended learning outcome and carry comparable workload. Lecturers shall not reward premium features that some students cannot obtain. Materials should be usable with reasonable bandwidth and compatible assistive technology. Where an outage affects a class, the lecturer must publish a consistent accommodation rather than leave each student to negotiate privately under time pressure.

6 Research publication and intellectual property

6.1 Research design and responsibility

AI-supported research shall document its purpose, data sources, methods, validation, limitations and foreseeable effects on participants and communities. The Principal Investigator and supervisor remain responsible for scientific integrity. Required data permissions, participant consent and institutional authorisations shall precede the relevant activity. Material changes to participants, privacy or methods shall be reviewed by the responsible project team and relevant authorised officers.

6.2 Evidence and reproducibility

Researchers shall verify every cited source and substantive extracted finding against the actual publication. AI-generated citations shall not enter the reference list without verification. Reviews shall describe searches, screening and extraction as performed; automated screening shall not be represented as independent human review.

Methods shall identify relevant software, model/version, prompts or configurations, data preparation and human validation. Code, statistical outputs and interpretation shall be checked against the study design and source data. Preserve original data and an auditable record of substantive changes. Synthetic data shall be clearly labelled and shall not be reported as collected observations.

6.3 Authorship disclosure and confidential review

AI tools shall not be listed as authors. Human authors remain accountable for accuracy, originality and integrity. Disclose the tool and how it was used in the manuscript and submission process as required; methods-related AI use belongs in the methodological account. These responsibilities align with ICMJE guidance, while BMU's October 2026 declaration rule applies across disciplines (International Committee of Medical Journal Editors, n.d.).

A reviewer shall not upload confidential manuscripts, theses, grant applications or appointment materials to an external AI tool without permission from the commissioning body and the required institutional safeguards. Research collaboration agreements shall specify data roles, permitted use and approval boundaries.

6.4 Rights and representations

Use of protected text, images, recordings, code and datasets shall comply with the Copyright Act, 2022, relevant licences and permissions. AI paraphrasing does not remove the obligation to credit the underlying source. Ownership or permission to reuse AI output shall not be assumed solely because a tool produced it (Federal Republic of Nigeria, 2022).

Generated images shall not be presented as documentary photographs, clinical findings or research observations. Preserve original images and record permitted transformations. The Legal Adviser shall resolve uncertain rights, licensing and contractual issues before publication, sharing or commercialisation.

7 Risk assessment and approval

7.1 Classification

The University AI Committee shall maintain four risk levels based on the proposed use, data, affected people, autonomy and consequences. The categories are BMU operational rules; NIST's framework supplies a general risk-management reference (Tabassi, 2023).

Level 1: limited assistance using public or genuinely non-sensitive information, with no consequential decision or external action. Use within a published approved category requires compliance and relevant training; a new application for every prompt is unnecessary.

Level 2: managed institutional use involving internal information, integrations or a substantial effect on educational or administrative processes. A named operational owner, documented testing, security review, relevant privacy assessment and a fallback are required.

Level 3: patient-facing use, identifiable health or research data, consequential assessment or employment/admission support, biometrics, or agents with significant system permissions. This requires a broader AI impact assessment, relevant specialist approvals, validation, a controlled pilot and written authorisation by the competent authority.

Level 4: prohibited or unlawful use, or use whose risks cannot be adequately controlled. It shall not be approved. Uncertain classification shall follow the higher relevant pathway pending review.

7.2 Application and decision

Submit a written proposal to the University AI Committee before acquiring, connecting or materially changing an institutional AI system. The committee

shall classify the proposal, arrange review and record the decision. Level 2 approval shall be issued only within written delegated authority; otherwise it shall be referred to the competent approving authority. Level 3 approval cannot be issued solely by the University AI Committee.

An approval shall specify the purpose, tool/configuration, permitted users and data, operational owner, restrictions, monitoring, expiry and review date. A pilot approval does not authorise unrestricted live use. Silence, a demonstration or purchase approval does not constitute operational authorisation.

The Head of ICT shall provide technical clearance. The Director of Academic Planning shall advise on privacy and applicable impact-assessment requirements. The Clinical Safety Lead shall provide clinical clearance where required. Missing specialist clearance is a reason to pause or redesign the proposal.

7.3 Validation change and retirement

Tests shall use predefined acceptance criteria and representative conditions, including difficult cases, foreseeable misuse, accessibility and subgroup limitations. High-risk evaluation requires appropriate independent challenge. Monitor errors, complaints, overrides and performance changes against approved thresholds.

A material change in model, purpose, data, population, hosting, integrations or autonomy requires reassessment before continued reliance. Review Level 3 approval at least annually and after a serious incident. Suspend unsafe functions promptly; record competent authorisation before restart.

On retirement, notify users, export required records, remove access and integrations, and document data return or deletion. The University AI Committee shall update the register and track closure. Retained records must remain sufficient to explain relevant decisions and research outputs.

8 Privacy, security and information management

8.1 Data protection

Processing shall comply with the Nigeria Data Protection Act, 2023 and applicable NDPC directives, including GAID 2025. Assess lawful basis, purpose limitation, minimisation, security, rights, transfers and retention. Consent is not a universal substitute for these requirements. The Director of Academic Planning shall identify applicable obligations and maintain the compliance schedule (Federal Republic of Nigeria, 2023; Nigeria Data Protection Commission, 2025).

Public AI services shall receive only public information or approved nonidentifying synthetic examples. Internal information requires an approved environment. Confidential student/staff records, unpublished assessments and protected research material require stricter access controls. Identifiable patient information, sensitive personal data, credentials and sensitive investigations require restricted handling. A paid account alone is insufficient protection.

Removing names does not necessarily anonymise information. Assess combinations of dates, locations, rare conditions and metadata; pseudonymised data remain controlled. Inputs, outputs, transcripts, retrieval stores, embeddings, logs and vendor copies shall all be covered by the assessment.

8.2 Privacy assessment and records

BMU requires a documented privacy impact assessment before institutional AI processing of personal data. The Director of Academic Planning shall advise on the legally required data protection impact assessment and any further notification or consultation.

Provide appropriate notices, assess overseas hosting and support access, control vendor training reuse and apply a records schedule. Preserve records needed for academic appeals, research, clinical care or legal obligations; delete unnecessary copies. A legal hold suspends routine deletion of relevant records.

The Director of Academic Planning shall coordinate rights requests and breach assessments. The records owner shall implement authorised retention and deletion. The University AI Committee shall monitor completion without receiving unnecessary patient information or confidential case details.

8.3 Technical controls and agents

The Head of ICT shall implement named-user access, least privilege, appropriate authentication, secure configuration, timely access removal, controlled integrations and protected credentials. Separate development and live environments; use approved test data and review code and dependencies before deployment.

Content retrieved from documents, websites or emails is untrusted input, not authority to change system instructions. Test for unintended disclosure and actions. Agents require explicit permission scopes and a competent human's approval of the actual proposed communication, record change, payment, deletion or access grant before execution.

Lost devices, compromised credentials or unauthorised integrations shall enter the incident pathway. Personal accounts shall not be the sole repository of University records. Export and closure arrangements shall address connected applications, tokens and vendor retention.

9 Clinical administrative and public use

9.1 Clinical education and patient care

Teaching simulations shall be separated from live care and labelled. A general-purpose chatbot shall not act as an independent diagnostic or treatment authority. Patient-facing use requires a named licensed professional, host institution authorisation and a documented clinical safety case. Students shall operate within their competence and supervision.

The Clinical Safety Lead shall oversee local validation, intended-use limits, stopping rules and clinical incidents. The Legal Adviser and Clinical Safety Lead shall determine applicable medical-device and professional regulatory requirements, including any NAFDAC requirements, before deployment. No regulatory exemption is presumed.

Patients shall receive understandable information about AI's role and relevant data use. Required consent and legal authority shall be documented. Clinical notes, summaries and transcriptions shall be checked before entering the authorised record. AI shall not independently prescribe, discharge or make emergency triage decisions. These safeguards follow the emphasis on human responsibility in WHO guidance (World Health Organisation, 2021, 2025).

9.2 Administration and procurement

Approved administrative assistance may support correspondence, planning and document handling. Responsible staff shall verify names, dates, amounts and rules before sign-off. Final employment and admission decisions remain with authorised people and bodies. Automated systems shall not covertly score staff productivity or replace fair consideration of evidence.

The Head of Procurement shall require a business case, total lifecycle cost, vendor due diligence, acceptance testing and exit arrangements. The Legal Adviser shall review contracts covering confidentiality, hosting, sub processors, training reuse, security, incident notice, audit evidence, rights assistance, ownership and data return/deletion. The Bursar shall maintain financial approval limits and segregation of duties.

9.3 Public communication

The University AI Committee shall coordinate AI-use declarations and factual verification for institutional reports. The Director of Academic Planning shall control publication of official messages. Verify claimed achievements, partnerships, health advice and emergency instructions against authorised records; correct material errors promptly.

Synthetic media that could be mistaken for an authentic recording shall be conspicuously labelled. Use of a person's image or voice requires appropriate permission. University chatbots shall identify themselves, use maintained approved information and offer a human route, especially for fees, admissions, welfare and clinical questions.

10 Inclusion training and continuity

10.1 Access and participation

The University AI Committee shall coordinate accessible guidance and support for staff and students. Required AI use shall account for cost, disability, language, device availability and connectivity. Essential services shall have a usable human or non-AI route. Personal diagnoses shall not be disclosed publicly to secure an accommodation.

The Head of Department shall arrange academic accommodations that preserve learning outcomes. Clinical and community projects shall examine re-identification, stigma and exclusion, including risks from small counts, maps or sensitive local knowledge. Community consultation does not replace individual rights or required consent.

10.2 Training

The University AI Committee shall organise induction on approved use, declarations, source verification, confidentiality, academic integrity and reporting. Lecturers, researchers, administrators and technical staff shall receive training relevant to their duties. Clinical users shall receive tool-specific training under the Clinical Safety Lead.

High-risk users shall demonstrate readiness before operational access. Material system changes and recurring incidents shall trigger refresher training. Completion and training scope shall be recorded. Users who require further preparation shall receive additional support and supervised practice.

10.3 Continuity and Bayelsa operating conditions

Essential services shall plan for flood disruption, power loss, connectivity failure and vendor outage, with site-specific evidence rather than assumed campus conditions. Each operational owner shall maintain a fallback communication route, restoration process and appropriate recovery objectives. Field teams shall have offline instructions and secure delayed synchronisation.

The Head of ICT and Director of Academic Planning shall assess equipment protection, backup separation and recovery capability. Test that records can

actually be restored. Designated staff shall reconcile duplicates, timestamps and conflicting records after reconnection; AI guesses shall not resolve source-data conflicts.

The Head of Department shall provide fair alternatives or extensions for documented disruption. Evidence requirements shall be proportionate to local conditions. The University AI Committee shall monitor access barriers and unresolved continuity actions. Procurement shall consider affordability, maintenance, energy use and disposal without unsupported environmental claims.

11 Incidents complaints and corrective action

11.1 Reporting and response

Report unsafe outputs, data exposure, impersonation, discriminatory effects, unauthorised actions, fabricated evidence and significant failures to the University AI Committee. Where immediate specialist action is needed, notify the Director of Academic Planning, Head of ICT or Clinical Safety Lead directly at the same time. Protect affected people and stop unsafe reliance before preparing a written account of the concern.

Serious harm, active compromise or sensitive-data exposure shall be reported immediately, with an internal target of one hour after discovery where safe communication is available. Other concerns shall be reported within one working day. Record outage-related delays honestly. Internal reporting targets do not replace or restart statutory or contractual notification periods.

The University AI Committee shall maintain the incident log and coordinate follow-up. The Head of ICT shall lead technical containment; the Clinical Safety Lead shall direct patient-safety action; and the Director of Academic Planning, with the Legal Adviser, shall assess and arrange required personal-data notifications within applicable legal deadlines. Do not delay a notification while awaiting a committee meeting.

11.2 Complaints and confidentiality

Staff, students and affected service users may request correction or human review through a written submission to the University AI Committee. The

committee shall acknowledge receipt within three working days and coordinate a substantive response within fifteen working days where practicable, or give reasons and a revised date. Protect good-faith reporters and retain records confidentially. Applicable statutory deadlines take precedence.

12 Implementation monitoring and review

12.1 Implementation from October 2026

The University AI Committee shall circulate this policy and the declaration requirements to all staff and students, publish current contact routes and maintain an accessible controlled copy. Electronic and paper communication routes shall be available through the responsible offices; unavailable internet access shall not prevent reporting.

During October 2026, departments shall report active institutional AI uses, identify their operational owners and flag unapproved high-risk activities. Unsafe or unlawful processing shall stop immediately. The inventory is a governance record and does not itself grant approval.

By the end of December 2026, the University AI Committee shall coordinate priority risk reviews, induction, the approved-tool register and revised assessment briefs. These administrative milestones do not postpone the October declaration requirement or immediate safety duties. Specialist clearances remain necessary before relevant deployments.

12.2 Registers assurance and reporting

Maintain a proportionate register of deployments, approvals, permitted data, operational owners, restrictions, review dates, status, incidents and corrective actions. Record departmental disclosure compliance through aggregate reports and sampled records; do not centrally collect every prompt or confidential research file.

Quarterly reports shall address declaration compliance, approval coverage, training, verified errors, incidents, complaints, access barriers, costs and overdue actions. State the reporting period, denominator, limitations and

responsible officer. Do not equate increased incident reporting with deteriorating conduct without considering improved awareness.

The Head of Internal Audit shall independently review selected high-risk approvals and compliance records. The University AI Committee shall track recommendations and escalate unresolved issues. A committee member who contributed to an activity shall not be its sole independent reviewer.

12.3 Exceptions and review

An exception shall specify its reason, risks, alternative safeguards, accountable officer and expiry, and shall receive approval from the competent authority. No exception may waive law, professional duties, prohibited uses or mandatory AI disclosure. Urgency does not justify uncontrolled deployment.

The University AI Committee shall coordinate annual review, first due in October 2027, and earlier review after significant incidents, legal changes or material operational concerns. Consult staff, students and relevant specialists. Substantive changes to duties or authority require approval through the University's established governance process; informal advice shall not amend the policy.