

**POLICY ON THE RESPONSIBLE USE AND DEPLOYMENT
OF
ARTIFICIAL INTELLIGENCE IN LEGAL EDUCATION
("LEGAL AI POLICY - LEAP")**

Applicable to Faculty, Students, Researchers and Staff

Prepared by

National Law University Delhi

Centre for Innovation Incubation and Entrepreneurship (CIIE)

NLU Delhi Foundation

September 2026

DOCUMENT CONTROL

Document title	Policy on the Responsible Use and Deployment of Artificial Intelligence
Policy custodian	AI Governance and Ethics Committee
Applies to	Students, faculty, research staff, administrative staff, centres, clinics, visiting scholars and persons representing the University
Review cycle	Annual, or earlier upon a change in law, judicial pronouncement or material technological development

TABLE OF CONTENTS

Executive Summary	3
PART I — PURPOSE, SCOPE AND PRINCIPLES.....	4
1. Purpose and Objectives	4
2. Scope and Application	4
3. Definitions	5
4. Governing Principles	6
5. Classification of Uses	7
6. Tiering of Artificial Intelligence Tools	7
PART II — ACADEMIC AND SCHOLARLY USE	9
7. Student Use and Assessment	9
8. Disclosure of Artificial Intelligence Assistance.....	9
9. Verification of Legal Authority.....	10
10. Faculty Use and Pedagogical Autonomy.....	11
11. Research, Publication and Supervision.....	12
12. Moots, Clinics and External Representation	12
13. AI-Assisted Evaluation and Feedback.....	13
PART III — DATA PROTECTION, SECURITY AND SYNTHETIC MEDIA.....	15
14. Data Protection Framework.....	15
15. Restricted Data and Anonymisation	17
16. Procurement and Vendor Obligations.....	18
17. Synthetic Media, Deepfakes and Digital Harms	18
PART IV — GOVERNANCE, COMPLIANCE AND ENFORCEMENT	20
18. AI Governance and Ethics Committee	20
19. Reporting and Investigation.....	20
20. Culpability and Sanctions.....	21
21. Review and Records	23
22. Training and AI Literacy.....	23
23. Commencement, Interpretation and Review	24
PART V — ANNEXURES	25
Annexure A — Classification of Permitted, Restricted and Prohibited Uses.....	25
Annexure B — Declaration of Artificial Intelligence Use	26
Annexure C — Citation Verification Log.....	27
Annexure D — Course Statement on Artificial Intelligence	28
Schedule of Authorities	29

EXECUTIVE SUMMARY

This Policy establishes a University-wide framework for the lawful, and ethical use of artificial intelligence at National Law University Delhi. It enables responsible adoption of AI in teaching, learning, research, clinical work and administration while protecting academic integrity, independent legal reasoning, confidentiality, personal data and institutional credibility.

The Policy proceeds from the single governing proposition that artificial intelligence may assist human work, but it may not replace human judgment. Every output produced with AI assistance remains, in full, the intellectual and professional responsibility of the person who submits, publishes or acts upon it. Responsibility cannot be delegated to a system, and it cannot be discharged by attributing an error to the technology.

The framework is risk-based. It classifies uses of AI as ordinarily permitted, permitted subject to controls, or prohibited. It tiers approved tools by the sensitivity of the data and the authority of the output. Further, it requires disclosure where AI assistance is material and it requires independent verification of every legal authority before that authority is cited or relied upon. Sanctions are graded by culpability, and every determination is subject to notice, hearing, reasons and appeal.

The Policy refers to the legal position established by the Supreme Court of India in *Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd.*, 2026 INSC 668, decided on 2 July 2026, in which the Court set aside orders of the National Company Law Tribunal and the National Company Law Appellate Tribunal that had rested upon non-existent, AI-generated precedents. The Court declared a position of zero tolerance for the production, citation or use of unverified AI-generated precedent, and held that a decision so contaminated is no decision in the eyes of the law even if only an iota of hallucinated material enters the decision-making process. For an institution that trains advocates, that standard is not a matter of external compliance; it is a matter of professional formation.

The Policy is further informed by the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, whose substantive obligations commence in phases; by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, which regulate synthetically generated information; and by the judicial approach of AI-generated fabrication in India and comparable jurisdictions.

Any unacknowledged content generated by AI within an assessment as though it is their own work will be considered as an academic misconduct. Transparency and accountability is the cornerstone of Responsible AI. The University's AI policy is based on the responsible use of AI by ensuring and allowing its stakeholders to use and integrate AI only after acknowledging the source and the nature of the AI tool.

PART I — PURPOSE, SCOPE AND PRINCIPLES

1. Purpose and Objectives

1.1 The University recognises that artificial intelligence is now embedded in legal research, legal practice, and scholarship, and that graduates of this University will practise in an environment shaped by it. The purpose of this Policy is therefore twofold: to enable the competent, confident and lawful use of artificial intelligence across the University, and to ensure that such use never displaces the independent reasoning that legal education exists to develop.

1.2 The objectives of this Policy are to protect academic integrity and the originality of scholarly work; to guarantee the accuracy of legal authority relied upon in work associated with the University; to safeguard personal data, confidential information and privileged communications; to preserve human accountability in every decision affecting the rights, marks, standing or interests of any person; to prevent the creation and circulation of deceptive synthetic media; and to build institutional capacity in AI literacy among students, faculty and staff.

1.3 This Policy is enabling in character. It does not prohibit responsible and ethical use of artificial intelligence.. It prohibits only those uses that undermine academic integrity and are deceptive, unsafe, unlawful, or destructive of the educational purpose for which assessed work is set.

2. Scope and Application

2.1 This Policy applies to all use of artificial intelligence in connection with the academic, research, clinical, co-curricular, representational or administrative activity of the University.

2.2 This Policy binds students of all programmes, faculty members, research staff, administrative and technical staff, visiting and adjunct faculty, research assistants and interns,

participants in University centres and clinics, and persons representing the University in external competitions, publications or engagements.

2.3 This Policy applies irrespective of whether the artificial intelligence system is accessed through University infrastructure, a University-licensed account, a personal account, an institutional subscription, an embedded feature of other software, or a freely available public service. The determining factor is the connection of the use to University work, not the ownership of the account or the device.

2.4 Where a course instructor, research supervisor, competition organiser, funding body, publisher or external partner imposes a stricter requirement than this Policy, the stricter requirement prevails for that work.

3. Definitions

3.1 In this Policy, unless the context otherwise requires:

- (a) “Artificial intelligence” or “AI” means a computational system that generates, predicts, classifies, summarises, analyses, ranks, or otherwise supports or produces decisions or content.
- (b) “Generative AI” means an artificial intelligence system that produces text, code, images, audio, video or other content in response to a prompt or instruction.
- (c) “Legal AI” means an artificial intelligence system designed for or applied to legal research, drafting, citation retrieval, compliance analysis, due diligence, litigation support, contract review or judicial analytics.
- (d) “Material AI assistance” means an AI contribution that substantively affects the ideas, arguments, structure, analysis, wording, evidence, data, code or conclusions of a work. Routine spelling correction, grammar checking, predictive text, reference formatting and translation of the user’s own prior text do not, without more, constitute material AI assistance.
- (e) “Hallucination” means output that is generated using AI or Generative AI or Legal AI but false, fabricated, unsupported, materially incomplete or misattributed, including non-existent judgments, invented citations, fabricated quotations, and paragraphs wrongly attributed to genuine authorities.
- (f) “Restricted data” means the categories of information specified in clause 15.2.

- (g) “Synthetically generated information” means audio, visual or audio-visual information that is artificially or algorithmically created or altered so as to appear authentic or to be reasonably indistinguishable from genuine information.
- (h) “Human-in-the-loop” means a process in which the owner of the AI generated work , verifies, interprets and adopts an AI-assisted output, exercises independent judgment upon it, retains the ability to override it, and accepts responsibility for the result.
- (i) “Committee” means the AI Governance and Ethics Committee constituted under clause 18.

4. Governing Principles

4.1 Human accountability. No artificial intelligence system may substitute for academic, professional, evaluative, disciplinary or administrative judgment. A person who submits, signs, publishes, files or acts upon an AI-assisted output is answerable for its entire content as though it were composed unaided.

4.2 Academic integrity. Artificial intelligence shall support the development of the user’s own understanding and shall not substitute for the intellectual contribution that a piece of assessed work is designed to elicit and to measure.

4.3 Transparency. Material AI assistance shall be disclosed in the manner prescribed by the instructor, supervisor, publisher, competition or this Policy. Disclosure made honestly and in good faith is not itself an admission of wrongdoing and shall not be treated as such.

4.4 Verification. The output of an artificial intelligence system is a draft, a lead or a hypothesis. It is never authority. Every legal proposition, citation, quotation, statutory provision, factual assertion and data point derived from or suggested by an AI system shall be independently verified against a primary or authoritative source before use.

4.5 Confidentiality and data protection. Restricted data shall not be entered into any artificial intelligence system that has not been approved for that category of data. Confidentiality obligations, legal professional privilege and the trust of clinic beneficiaries are not suspended by the convenience of a tool.

4.6 Fairness and non-automation of consequential decisions. No decision that materially affects a person’s marks, progression, employment, standing, welfare or disciplinary position shall be taken solely by automated means.

4.7 Proportionality. Institutional controls, investigative measures and sanctions shall be proportionate to the risk, the degree of culpability, the scale of the conduct and the harm caused.

4.8 Equity of access. The University shall have regard to disparities in access to paid AI tools, and shall not design assessment or research requirements in a manner that advantages those able to purchase superior systems.

4.9 Responsible innovation. Experimentation with artificial intelligence is encouraged where it is documented, supervised, conducted on appropriate data, and fit for the purpose to which it is applied.

5. Classification of Uses

5.1 Uses of artificial intelligence are classified as ordinarily permitted, permitted subject to controls, or prohibited, in accordance with Annexure A.

5.2 A use that is ordinarily permitted remains subject to any contrary rule set by the instructor for a particular course or assessment, and remains subject in every case to the verification requirement in clause 9.

5.3 A use that is permitted subject to controls requires disclosure under clause 8, verification under clause 9, and the exercise and recording of independent human judgment upon the output.

5.4 A prohibited use is not rendered permissible by disclosure. Disclosure is a condition of legitimate use; it is not a licence for conduct that is otherwise impermissible.

6. Tiering of Artificial Intelligence Tools

6.1 Artificial intelligence tools are tiered by the assurance available in respect of their security, data handling and source fidelity, in accordance with the table below. The Committee shall maintain and publish a register of tools assigned to each tier.

Tier	Description and permitted use
Tier 1 — Approved legal research systems	Source-linked legal research tools operating on authorised legal databases within an approved environment. Permitted for legal research and for restricted data expressly authorised for that tool. Independent verification under clause 9 remains mandatory.

Tier 2 — Approved enterprise systems	Systems contracted by the University with contractual privacy, security and retention controls. Permitted for drafting, structuring, summarisation and analysis, and for restricted data expressly authorised for that tool. Not authoritative as to legal citation.
Tier 3 — Public or unassessed systems	Publicly available systems adopted without institutional assessment. Permitted only for low-risk preliminary assistance on non-restricted material. Prohibited for restricted data, for the identification of authority relied upon without verification, and in any assessment in which use is not permitted.

6.2 No tool shall be used with restricted data unless it has been assigned to Tier 1 or Tier 2 and approved for that category of data.

6.3 The assignment of a tool to Tier 1 does not dispense with the verification requirement in clause 9. Tier 1 tools may provide links to, or retrieve information from, recognised legal databases and other authorised sources, but the presence of a source link does not by itself establish that the information provided by the tool is correct or that it accurately represents the source. A tool may, for example, identify the wrong case, rely on an outdated or superseded authority, misstate the legal proposition contained in a judgment, or incorrectly summarise or quote the source. Accordingly, students and other users must still locate and read the original or authoritative source and independently verify the authority, proposition, quotation and its current legal status before relying upon it. Source-linking reduces, but does not completely eliminate, the risk of misattribution, superseded authority and incorrect summarisation.

PART II — ACADEMIC AND SCHOLARLY USE

7. Student Use and Assessment

7.1 Every course outline shall specify one of three modes for each assessment, and shall communicate that mode to students before the assessment is set:

- (a) AI-Prohibited: no use of artificial intelligence is permitted in the preparation or production of the work.
- (b) AI-Limited: specified uses are permitted, subject to disclosure; all other uses are prohibited.
- (c) AI-Integrated: use of artificial intelligence is permitted and may form part of what is assessed, subject to disclosure and to the verification requirement.

7.2 Where a course outline is silent, the AI-Limited mode shall apply, and the permitted uses shall be those classified as ordinarily permitted in Annexure A.

7.3 Artificial intelligence shall not be used in any examination, viva voce, timed assessment, invigilated test or closed-book exercise unless its use is expressly authorised in writing for that assessment.

7.4 In all assessed work, students shall follow the Read–Verify–Reason sequence. The student shall read the primary materials directly; shall independently verify every proposition, authority and factual claim; and shall reason, structure and express the analysis in the student's own words. Work that reproduces AI output with superficial modification does not satisfy this requirement, irrespective of whether the output is accurate.

7.5 A student who is uncertain whether a proposed use of artificial intelligence is permitted shall seek clarification from the instructor before using it. A student who seeks and follows such clarification in good faith shall not be subject to sanction in respect of that use.

8. Disclosure of Artificial Intelligence Assistance

8.1 Where artificial intelligence has provided material AI assistance to a submitted or published work at NLUD under any research project submitted by the student or submitted for publication to NLUD journals or any other research project of the University, the person submitting or publishing it shall disclose the tool used, the purpose for which it was used, and the extent of its contribution.

8.2 Disclosure shall be made in the form set out in Annexure B, or in such other form as the instructor, supervisor or publisher requires.

8.3 The following model statement satisfies clause 8.1 in the ordinary case: “The author used [tool] for [purpose]. All authorities, quotations, factual claims, data, analysis and conclusions have been independently verified and are adopted as the author’s own.”

8.4 Artificial intelligence shall not be named as an author or co-author of any work. Authorship entails accountability, which an artificial intelligence system cannot bear under the present policy.

8.5 A disclosure that is materially false or materially incomplete is itself a breach of this Policy and will entail the same punishment as that of undisclosed use of AI.

9. Verification of Legal Authority

9.1 No authority or scholarship shall be cited, quoted or relied upon in any work associated with the University unless it has been located, read and independently verified from a primary or authoritative source by the person relying upon it.

9.2 This rule gives effect to the standard articulated by the Supreme Court of India in *Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd.*, 2026 INSC 668, in which the Court set aside the orders of the National Company Law Tribunal and the National Company Law Appellate Tribunal on the ground that the adjudication had rested upon non-existent judgments and upon AI-generated paragraphs wrongly attributed to genuine citations. The Court declared zero tolerance, for the Bar as well as the Bench, for citing, referring to or relying upon such material, and held that a decision affected by such material is no decision in the eyes of the law, irrespective of whether the material had a direct or indirect bearing on the outcome, and is liable to be set aside even if an iota of fake or hallucinated material entered the decision-making process. The Court further directed the Bar Council of India to constitute a committee to deliberate upon the submission of fabricated material by members of the Bar.

9.3 Students of this University enter a profession in which the citation of an unverified authority is now a matter of professional discipline. The verification requirement is accordingly a requirement of professional formation and not merely of academic hygiene.

9.4 Verification protocol: Verification requires four steps, each of which must be completed:

- (a) Locate - Retrieve the authority from an official court record, an official gazette, or an authorised legal database. Retrieval of a reference from an AI system, a secondary summary or a search result snippet is not location.
- (b) Read - Examine the judgment, statute or source itself, and not solely a headnote, summary or extract.
- (c) Match - Confirm the parties, the court, the coram, the date, the citation, the paragraph relied upon, the accuracy of any quotation, the proposition attributed to the source, and the current status of the authority, including whether it has been overruled, stayed, distinguished or superseded.
- (d) Record - Enter the source consulted, the date of verification and the paragraphs relied upon in the Citation Verification Log at Annexure C, where such a log is required under clause 9.6.

9.5 A citation shall be treated as unverified, and shall not be used, where the authority cannot be located in any authorised database or official record; where the citation format is internally inconsistent or the volume, year or page is implausible; where the quoted passage cannot be found in the text of the judgment; where the proposition attributed to the authority is not borne out on reading it; or where the AI system, when asked, alters or withdraws the citation.

9.6 A Citation Verification Log shall be maintained for dissertations, theses, work submitted for publication, memorials and written submissions filed in external competitions, student research projects, research produced under University centres, and any work in which the instructor or supervisor requires one.

9.7 Responsibility for verification rests with the Author of the work. Where work is co-authored, each author is responsible for the authorities cited in the portions attributed to that author, and the corresponding or lead author is responsible for the integrity of the whole.

10. Faculty Use and Pedagogical Autonomy

10.1 Faculty members retain autonomy to determine the role of artificial intelligence in their courses, and may permit, restrict or prohibit its use for any assessment, provided that the position adopted is communicated to students in advance and applied consistently.

10.2 Artificial intelligence may be used by faculty for preparation of teaching materials, literature mapping, drafting, coding, data analysis, translation, administrative correspondence and the generation of practice questions, subject to this Policy.

10.3 Artificial intelligence shall not be used to determine a mark, to evaluate a dissertation or thesis, to make a finding of misconduct, or to decide any matter of admission, employment, welfare or discipline, otherwise than in accordance with clause 13.

10.4 A faculty member who uses artificial intelligence in the preparation of teaching or assessment materials remains responsible for the accuracy of those materials, including the accuracy of every authority stated in them.

11. Research, Publication and Supervision

11.1 Use of artificial intelligence in research shall be disclosed in accordance with the requirements of the publisher, funder or supervisor, and in any event in accordance with clause 8.

11.2 Artificial intelligence shall not be used to fabricate, augment, interpolate or selectively generate empirical data, interview material, survey responses or case records. Synthetic data may be used only where its use is disclosed, methodologically justified and approved by the supervisor or the relevant research ethics process.

11.3 Unpublished manuscripts, peer-review materials, confidential research data and identifiable human-subject data shall not be entered into any system other than an approved Tier 1 or Tier 2 tool authorised for that data.

11.4 A supervisor shall satisfy himself or herself that the scholar can independently explain, defend and reconstruct the reasoning and the sources of the work supervised. The capacity to explain the work is the operative test of authorship.

11.5 Research assistants shall be informed in writing of the AI-related requirements applicable to the project on which they are engaged, before commencing work.

12. Moots, Clinics and External Representation

12.1 A heightened standard applies to work carried out in the name of the University before an external forum, including moot court competitions, arbitration and mediation competitions, client counselling, negotiation, judgment writing, policy competitions, legal aid clinics and external publications.

12.2 Subject always to the rules of the competition or forum concerned, artificial intelligence may be used for brainstorming, issue identification, research planning, language refinement and formatting.

12.3 Artificial intelligence shall not be used to generate the substantive text of a memorial, written submission, opinion or oral script; to identify authorities that are then cited without independent verification; to process a confidential competition problem, clinic file or beneficiary information in an unapproved system; or to provide any assistance during a round, hearing or interview in which such assistance is not permitted.

12.4 Clinic work involving identifiable beneficiaries, case files, witness information, litigation strategy or privileged communications shall not be processed through any system other than an approved tool authorised for that data. The obligation of confidentiality owed to a legal aid beneficiary is not diminished by the beneficiary's inability to enforce it.

12.5 Before any submission is filed or sent externally in the name of the University, the participant and the supervising faculty member shall certify that every authority has been independently verified and that the use of artificial intelligence complied with the rules of the forum and with this Policy.

13. Guidance for Examiners

13.1 Examiners shall not upload, copy, paste, submit, or otherwise disclose student submissions, examination scripts, answer scripts, dissertations, research papers, assignments, memorials, or any other student-generated work to publicly available or unapproved Generative AI tools or Large Language Models for the purpose of assessment, evaluation, grading, moderation, or feedback.

13.2 The evaluation of student work, including the determination of marks, grades, academic merit, and qualitative assessment, shall remain the responsibility of the examiner. AI tools shall not be used as a substitute for the examiner's professional and academic judgment.

13.3 Where the use of an approved AI tool is permitted for assisting in the preparation or refinement of feedback, the examiner shall use the tool only in a manner consistent with this Policy and applicable data-protection requirements. Such use shall preferably be based on the examiner's own notes, observations, or independently formulated feedback rather than on the

direct submission of the student's work. The examiner shall review, verify, and take responsibility for the final feedback before it is communicated to the student.

13.4 Examiners shall have particular regard to the confidentiality, privacy, intellectual-property rights, and other interests associated with student submissions. No student work shall be entered into an AI system unless the relevant system has been expressly approved for such use by the University and the use is consistent with the applicable data-handling requirements under this Policy.

13.5 Examiners shall not treat an AI-detection tool or an AI-generated probability or score, by itself, as conclusive evidence that a student has used AI in breach of this Policy. Where concerns arise regarding possible unauthorised use of AI, the matter shall be dealt with in accordance with the University's applicable academic-integrity and disciplinary procedures, with appropriate human review and supporting evidence.

13.6 Faculty members and examiners involved in the design or review of assessments should, where appropriate, consider whether the assessment requires students to demonstrate knowledge, reasoning, analysis, application, reflection, or other skills that cannot be adequately established merely through AI-generated output. Assessment instructions should clearly communicate whether, and to what extent, AI tools may be used for the particular assessment.

13.7 Examiners shall assess student work in accordance with the applicable assessment brief, course requirements, and this Policy. Where AI use has been expressly permitted for an assessment, the examiner shall not penalise a student merely for permissible use of AI, but may take into account the manner and extent of such use where these form part of the stated assessment requirements.

13.8 Where an examiner reasonably suspects that a student has used AI in a manner prohibited by the assessment instructions or this Policy, the examiner shall not attempt to establish the matter solely through an AI-detection tool. The concern shall instead be documented and referred through the University's prescribed academic-integrity process.

PART III — DATA PROTECTION, SECURITY AND SYNTHETIC MEDIA

14. Data Protection Framework

14.1 The Digital Personal Data Protection Act, 2023 governs the processing of digital personal data. The Digital Personal Data Protection Rules, 2025, were notified on 13 November 2025 and provide for commencement in phases, with the substantive obligations concerning notice, consent, reasonable security safeguards, intimation of personal data breach, retention and cross-border processing taking effect eighteen months from 14 November 2025.

14.2 The University does not treat the phased commencement of those obligations as a reason to defer good practice. This Policy is framed to achieve institutional readiness in advance of the commencement date, and the standards set out in this Part apply from the commencement of this Policy.

14.3 All processing of personal data in connection with artificial intelligence shall be undertaken only for a defined and permitted institutional purpose and in accordance with the following standards:

(a) For the purposes of this Policy, the **University shall be treated as the Data Fiduciary** in respect of personal data processed for purposes determined by the University, including academic administration, teaching and learning, assessment, research administration, recruitment, employment, institutional governance, student services and other legitimate institutional functions. The University shall determine the purpose and means of such processing and shall be responsible for establishing appropriate safeguards and controls governing the use of personal data in AI systems.

(b) Where an external AI provider, technology vendor, cloud service provider or other third-party processes personal data on behalf of the University and in accordance with the University's instructions, such entity shall be treated as a **Data Processor** for the purposes of this Policy. The engagement of a Data Processor shall be subject to appropriate contractual, technical and organisational safeguards, including requirements concerning confidentiality, security, permitted use, retention, deletion and prevention of unauthorised reuse of personal data.

(c) Personal data may be processed through an AI system only where such processing is necessary for, and proportionate to, a specified and lawful purpose authorised by the University.

Permitted processing may include, where expressly authorised and appropriately safeguarded, activities such as administrative assistance, academic support, assessment-related functions, research support, drafting, analysis, summarisation or other institutional purposes identified by the University. Personal data shall not be processed merely because an AI system is capable of processing it. Student records collected for academic administration, for example, shall not be used to test prompts, evaluate AI tools or develop workflows unless such processing has been separately authorised and is consistent with applicable data-protection requirements.

(d) Personal data shall be processed only for the specified purpose for which the processing has been authorised. Data collected for one institutional purpose shall not be repurposed for AI experimentation, system testing, model training or other unrelated purposes without appropriate authorisation.

(e) Only such personal data as is necessary for the specified and authorised purpose shall be processed. Where the intended purpose can reasonably be achieved without identifying information, anonymised or appropriately de-identified information should be used instead.

(f) The accuracy of an AI-generated output shall not be assumed merely because the output is fluent, plausible, or generated by an approved or reputable system. Where an AI output is used in University work and contains factual, academic or legal assertions, the responsible user shall undertake appropriate independent verification in accordance with clause 9.4.

(g) Personal data shall not be retained within an AI system for longer than is necessary for the authorised purpose. Features permitting indefinite retention, reuse, training on inputs, or use of University data for purposes beyond the authorised processing shall be disabled or otherwise controlled unless expressly approved by the University.

(h) Appropriate technical and organisational safeguards shall be applied to personal data processed through AI systems, including access controls, encryption in transit and at rest where available and appropriate, logging, authentication, and other safeguards proportionate to the nature and sensitivity of the data.

15. Restricted Data and Anonymisation

15.1 Institutional rule. No member of the University community shall enter restricted data into any artificial intelligence system that has not been expressly approved for that category of data.

15.2 The following are restricted data:

- (a) Student information, including academic records, marks, transcripts, attendance, disciplinary records, examination content prior to release, scholarship and financial assistance records, and accommodation or support records.
- (b) Employee information, including personnel files, recruitment records, performance assessments and remuneration details.
- (c) Research information, including identifiable human-subject data, interview transcripts, unpublished findings, confidential datasets and materials received under a confidentiality undertaking.
- (d) Clinic and legal aid information, including the identity of beneficiaries, case files, witness statements, litigation strategy, settlement material and any privileged communication.
- (e) Identity and financial information, including identity document numbers, bank and payment details, and authentication credentials.
- (f) Institutional information, including unreleased examination papers, marking schemes, internal legal advice, security configurations and contractual material subject to confidentiality.

15.3 Anonymisation. Removal of a name does not anonymise a record. A record remains identifiable where a person can be recognised from a combination of attributes such as age, locality, dates, institutional role, procedural history or distinctive facts/fake attributes. Anonymization shall address the risk of indirect identification, and shall be assessed before, not after, the record is entered into any system.

Illustration. A clinic note recording that a woman of a stated age from a named locality filed a complaint of a specified nature on a specified date remains identifiable notwithstanding the deletion of her name, because the residual combination of attributes is sufficient to identify her within a small population. Such a record shall not be entered into an unapproved system in that form.

15.4 Where a member of the University community becomes aware that restricted data has been entered into an unapproved system, that person shall report the fact promptly to AI Governance & Ethics Committee.

16. Procurement and Vendor Obligations

16.1 Before an artificial intelligence tool is adopted at institutional level or assigned to Tier 1 or Tier 2, it shall be assessed for the purpose and categories of data involved, the security controls available, the retention and deletion arrangements, the use of sub-processors, the location of processing, the availability of audit and termination rights, and its accuracy and accessibility characteristics.

16.2 Agreements and Memorandums of Understanding (MoUs) for the supply of artificial intelligence services shall provide that University data shall not be used to train or improve the supplier's models without express written approval; shall specify security obligations, retention periods and deletion on termination; shall require disclosure of sub-processors; shall require notification of any personal data breach; and shall permit suspension and termination for non-compliance.

16.3 No individual member of the University community shall bind the University to the terms of an artificial intelligence service, whether by accepting terms of use, uploading institutional data, or enabling institutional access, save in accordance with the University's ordinary authorisation processes.

17. Synthetic Media, Deepfakes and Digital Harms

17.1 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 16 February 2026 and effective from 20 February 2026, introduce a regulatory framework for synthetically generated information, requiring that such information be labelled prominently and be traceable, and imposing accelerated obligations upon intermediaries in respect of unlawful synthetic content.

17.2 Any member of the University community who creates or disseminates synthetically generated information in connection with University activity, including for teaching, illustration, research, advocacy training or promotion, shall label it clearly and conspicuously as artificially generated. A label shall not be removed, obscured or rendered ineffective.

17.3 The following are prohibited absolutely: the creation or dissemination of synthetic media intended or likely to deceive as to authenticity; the impersonation of any person by synthetic

audio, image or video; the fabrication of a communication, document, record or item of evidence; the generation of sexual or intimate imagery of any person without consent; targeted harassment, abuse, disclosure of private information or defamation effected through AI-generated content; and the use of artificial intelligence to generate malicious code or instructions for circumventing security controls.

17.4 The prohibition in clause 17.3 applies to synthetic media concerning members of the University community and to synthetic media concerning any other person, and applies whether or not the material is created on University premises or infrastructure.

17.5 Reporting and response. A person affected by conduct falling within clause 17.3 may report it through the designated reporting channel. Reports shall be handled confidentially. The University shall, on receipt of a report, take steps to preserve evidence, assess the immediate safety of the person affected, assist with requests for removal of the material, and provide access to support.

17.6 Investigative restraint. Any examination of a personal device or personal account in the course of an investigation requires either the informed consent of the person concerned or lawful authority. Where such an examination is undertaken, it shall be limited to a scope recorded in writing in advance, shall use the least intrusive means available, shall segregate and disregard unrelated material, shall be conducted with a witness present, and shall be documented. Refusal to consent shall not, of itself, be treated as evidence of the conduct alleged.

17.7 Where conduct may constitute a criminal offence, the University shall preserve the evidence and, where appropriate, refer the matter to the competent authorities. The University shall not compel the disclosure of passwords, the production of a confession, or unrestricted access to a personal device.

PART IV — GOVERNANCE, COMPLIANCE AND ENFORCEMENT

18. AI Governance and Ethics Committee

18.1 It is proposed to constitute an AI Governance and Ethics Committee, by the competent authority, which may comprise of faculty members, expert(s) in information technology function, a representative of the library and research services, a student representative, and such external expert members as the competent authority considers appropriate.

18.2 The functions of the Committee are to maintain this Policy and to recommend amendments; to maintain and publish the register of approved tools and their tier assignments; to assess proposals for institutional adoption of artificial intelligence tools; to issue interpretive guidance and model clauses for course outlines; to oversee training under clause 22; to receive reports of incidents and to analyse patterns arising from them; and to report annually to the competent authority on the operation of this Policy.

18.3 The Committee does not determine allegations of misconduct against individuals, and shall not perform an adjudicatory function in respect of any person.

19. Reporting and Investigation

19.1 A concern regarding a breach of this Policy may be raised by any member of the University community through the designated reporting channel.

19.2 Where a concern relates to a submitted piece of work, it shall in the first instance be considered by the instructor or supervisor, who may resolve a matter falling within Category I of clause 20 by counselling, correction and resubmission without further process.

19.3 Where a matter is not so resolved, it shall be referred for inquiry. The inquiry shall observe the following requirements:

- (a) Preservation - The work, its bibliography, any disclosure statement, any citation verification log and any available version history shall be preserved.
- (b) Source audit - A reasoned sample of the authorities cited shall be independently verified. Where errors are found in the sample, the audit shall be widened.
- (c) Evidence - Findings shall rest upon verifiable evidence, being the existence or nonexistence of the authorities cited, the accuracy of quotations, the correspondence between the work and the sources claimed, the disclosure made, and the person's ability to explain the reasoning and sources of the work.

(d) Notice - The person concerned shall be informed in writing of the allegation and of the material relied upon, and shall be afforded a reasonable opportunity to respond, to explain the research process followed, and to produce the sources consulted.

(e) Reasons - The determination shall be recorded in writing with reasons, identifying the evidence relied upon and the findings made on the balance of probabilities.

19.4 Limits of detection software - The output of a tool that purports to detect AI-generated text is not evidence of misconduct and shall not, alone or principally, form the basis of any finding. Such tools produce false positives, and are documented to do so disproportionately in respect of writers who use English as an additional language and writers whose prose is formulaic by reason of training or subject matter. Nor shall inference be drawn from stylistic impression, vocabulary, fluency, or the absence of characteristic error.

19.5 The inability of a person to explain the reasoning, structure or sources of work submitted as that person's own is relevant evidence and may be relied upon.

20. Culpability and Sanctions

20.1 Sanctions under this Policy are graded by culpability and are not automatic. The category into which conduct falls shall be determined on the evidence, and the sanction shall be determined within that category having regard to the factors in clause 20.4.

Category	Nature of conduct	Ordinary range of sanction
Category I Inadvertent lapse	An isolated citation or reference error with no material effect on the analysis; a minor omission in disclosure made otherwise in good faith.	Counselling; correction and resubmission; a direction to complete training. No adverse record.
Category II Negligent reliance	Failure to verify authority resulting in material inaccuracy; material AI assistance not disclosed where disclosure was required; use exceeding the permitted mode without concealment.	Reduction in marks; formal written warning; mandatory training; a direction to resubmit.

Category III Reckless misuse	Substantial undisclosed reliance on AI output in place of the person's own work; repetition of Category II conduct after warning; conduct that conceals the extent of assistance.	Substantial reduction in marks or failure of the component; formal record of misconduct; removal from a research or representative role; probation.
Category IV Fabrication and deception	Knowingly citing an authority understood to be non-existent or unverified; fabrication of evidence, data or quotation; substitution of AI output for the person's own work in its entirety; deceptive synthetic media; falsification of a disclosure or a verification log.	Nil marks for the work; failure of the course; withdrawal of representation of the University; recommendation of suspension or such other sanction as may lawfully be imposed.

20.2 A person shall not be found to have engaged in deliberate deception by reason only of the presence of an inaccurate citation. A finding of deliberate fabrication requires evidence of knowledge or of a conscious disregard of the obvious.

20.3 Conversely, a failure to verify is not excused by the assertion that an artificial intelligence system produced the error. The obligation to verify is personal, and its breach is the negligence in question. The distinction drawn by this Policy is between a person who failed to check and a person who knew, and it goes to the gravity of the sanction rather than to the existence of the breach.

20.4 In determining the sanction, the decision-maker shall have regard to the degree of intent; the extent of the material affected; the stage of study or seniority of the person concerned; whether the use was disclosed; whether the work was submitted externally or in the name of the University; the harm caused or risked; any prior finding; the promptness and candour of any admission; and the corrective steps taken.

20.5 Voluntary disclosure of a breach before it is detected, and prompt cooperation with any inquiry, shall be treated as substantial mitigation.

20.6 Where the conduct is attributable in part to inadequate instruction, ambiguity in the course outline, or the absence of any stated position on the use of artificial intelligence for the assessment concerned, that shall be taken into account in mitigation.

21. Review and Records

21.1 A person in respect of whom a determination is made under clause 20 shall be informed in writing of the determination, the reasons for it, the sanction imposed and the right to seek review.

21.2 A review may be sought on the grounds that the process was not observed, that relevant material was not considered, that the finding was not reasonably open on the evidence, or that the sanction was disproportionate. The review shall be conducted by a person who was not involved in the original determination.

21.3 Records of determinations shall be retained securely, shall be accessible only to those with a legitimate institutional need, and shall be retained for such period as the University determines and no longer.

21.4 A matter shall be reported to an external body only where the University is required by law to do so or is separately authorised to do so.

22. Training and AI Literacy

22.1 The University shall provide recurring training at least once a semester (in the beginning of the semester) on the responsible use of artificial intelligence, covering the capabilities and limitations of these systems, the mechanics of citation verification, data protection and confidentiality, bias and fairness, synthetic media, research integrity, and the approved tools available.

22.2 Training shall be provided to students at the commencement of the programme and shall be reinforced before the first substantial research submission.

22.3 Faculty members and staff shall be offered training appropriate to their functions, including guidance on framing course-level positions on the use of artificial intelligence.

22.4 Role-specific orientation may be required of research assistants, clinic participants, competition teams and administrative staff handling restricted data.

23. Commencement, Interpretation and Review

23.1 This Policy takes effect on the date on which it is approved by the competent authority of the University.

23.2 The Committee shall review this Policy at least once in every academic year, and earlier where required by a change in law, a judicial pronouncement, or a material development in the technology.

23.3 A question as to the interpretation of this Policy shall be referred to the Committee, which may issue guidance. Guidance issued under this clause is subordinate to the Policy and shall not extend or diminish its requirements.

23.4 If any provision of this Policy is inconsistent with applicable law, that provision shall be read so far as possible in conformity with the law, and to the extent that it cannot be so read, the law shall prevail and the remaining provisions shall continue in effect.

PART V — ANNEXURES

Annexure A — Classification of Permitted, Restricted and Prohibited Uses

This Annexure is referred to in clause 5. It is illustrative and not exhaustive. Where a use is not addressed, the governing principles in clause 4 apply.

Classification	Illustrative uses
Ordinarily permitted	Explanation of concepts and doctrines; generation of search terms and research strategies; brainstorming and issue identification; grammar, style and clarity refinement of the user's own text; formatting and reference styling; translation of the user's own text; generation of practice questions; summarisation of material the user has read, for the user's own comprehension.
Permitted subject to disclosure, verification and human approval	Structuring of research outlines; literature mapping; substantial drafting assistance; code generation and data analysis; assistance with dissertations, theses and publications; preparation of teaching material; administrative drafting; decision support in administrative processes.
Prohibited	Submission of AI-generated work as the person's own; use in any assessment in which use is not permitted; citation of authority that has not been independently verified; fabrication of authority, evidence, data or quotation; entry of restricted data into an unapproved system; generation of a mark or evaluative determination without human review; creation or dissemination of deceptive synthetic media; impersonation; generation of malicious code or means of circumventing security controls; falsification of a disclosure or verification log.

Annexure B Declaration of Artificial Intelligence Use

This Annexure is referred to in clause 8. It shall accompany any submission in which artificial intelligence provided material assistance.

Name of person submitting: _____

Programme / Department: _____

Title of work: _____

Course and assessment (where applicable): _____

1. Artificial intelligence tool or tools used: _____
2. Purpose for which each tool was used: _____
3. Extent of the contribution of each tool: _____

I declare that:

- (a) the disclosure above is complete and accurate;
- (b) I have independently located, read and verified every authority, statutory provision, quotation, factual claim and data point relied upon in this work;
- (c) no restricted data was entered into any system not approved for that data;
- (d) the analysis, structure and expression of this work are my own, and I am able to explain and defend its reasoning and sources; and
- (e) I accept full responsibility for the entire content of this work.

Signature: _____ Date: _____

Annexure C Citation Verification Log

This Annexure is referred to in clause 9.6. A separate entry shall be made for every authority relied upon. The log shall be produced on request.

No.	Authority and citation	Source consulted	Paragraphs	Proposition or quotation verified	Date of verification
1					
2					
3					
4					
5					

Name of verifier: _____

Signature: _____

Date: _____

Annexure D: Course Statement on Artificial Intelligence

This Annexure is referred to in clause 7.1. Instructors shall include a completed statement in the course outline for each course.

Course: _____

Instructor: _____

1. Mode applicable to this course (indicate for each assessment): AI-Prohibited ☐ AI-Limited ☐ AI-Integrated ☐

2. Uses expressly permitted in this course:

3. Uses expressly prohibited in this course:

4. Disclosure required: Yes ☐ No ☐

Form of disclosure: _____

5. Citation Verification Log required: Yes ☐ No ☐

6. Is any AI tool used to assist evaluation or feedback in this course?

Yes ☐ No ☐

If yes, state the tool, its purpose, the data it processes, its limitations, and the process by which a student may seek review:

7. Students may seek clarification regarding the use of artificial intelligence in this course from:

SCHEDULE OF AUTHORITIES

A. Legislation and Subordinate Legislation

1. Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
2. Digital Personal Data Protection Rules, 2025, notified 13 November 2025, providing for phased commencement.
3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified 16 February 2026, effective 20 February 2026.

B. Judicial Decisions

1. Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd., 2026 INSC 668 (Supreme Court of India, Narasimha and Aradhe JJ., 2 July 2026) — orders of the National Company Law Tribunal and the National Company Law Appellate Tribunal set aside for reliance upon non-existent, AI-generated precedents; zero tolerance declared for the Bar and the Bench; Bar Council of India directed to constitute a committee.
2. Christian Louboutin SAS v. M/s The Shoe Boutique – Shutiq, Delhi High Court, 22 August 2023 (Prathiba M. Singh J.) — responses of a generative AI system cannot form the basis of adjudication; artificial intelligence cannot substitute either human intelligence or the humane element in the adjudicatory process.
3. Jaswinder Singh v. State of Punjab, CRM-M-22496-2022, Punjab and Haryana High Court, 27 March 2023 (Chitkara J.) — reference to a generative AI system in the course of a bail proceeding, the Court expressly recording that the reference was neither an expression of opinion on the merits nor a matter to be adverted to by the trial court.
4. Anil Kapoor v. Simply Life India and Others, CS(COMM) 652/2023, Delhi High Court, 20 September 2023 — injunction restraining the use of artificial intelligence to generate imagery, voice and likeness of an individual without consent.
5. KMG Wires Private Limited v. National Faceless Assessment Centre, Writ Petition (L) No. 24366 of 2025, Bombay High Court, 26 October 2025 (Colabawalla and Jamsandekar JJ.) — income tax assessment order set aside for reliance upon non-existent case law, the Court observing that results generated by such systems are not to be blindly relied upon but must be duly cross-verified before use.

6. *Buckeye Trust v. Principal Commissioner of Income Tax*, Income Tax Appellate Tribunal, Bengaluru — order recalled upon discovery that authorities relied upon were fabricated.
7. *Ayinde v. London Borough of Haringey*; *Al-Haroun v. Qatar National Bank QPSC*, [2025] EWHC 1383 (Admin) (Divisional Court) — consideration of the professional consequences of placing fabricated authorities before a court.
8. *Mata v. Avianca Inc.*, 678 F. Supp. 3d 443 (S.D.N.Y. 2023) — sanctions imposed for the submission of fabricated judicial opinions produced by a generative AI system.

Each authority listed in this Schedule was independently located and verified against a primary or authoritative source in the course of preparing this Policy, in accordance with clause 9.