Academic Integrity, Artificial Intelligence, Online Assessment and VLE Use Policy

Supplemental Institutional Policy

POLICY # EAI/2026/260401

Approved by the Senate on April 1, 2026.

This policy supplements existing approved policies and does not replace them.

Policy Number	EAI/2026/260401
Version	1.0
Status	Approved by the Senate on April 1, 2026
Owner	Quality Assurance Cell
Responsible Office	Dean of Quality Assurance, Controller of Exams, Learning Design Support Office and Data Protection Officer
Applies To	Students, academic staff, administrative staff, technical staff, online delivery partners and approved support service partners
Review Cycle	Annual review or earlier where required by MFHEA, GDPR, technology change, AI regulation or institutional need

Euro American Institute

AGORA BUSINESS CENTRE LEVEL 2
TRIQ IL WIED TA' L IMSIDA
MSIDA, MSD 9020, MALTA
qa@euroamerican.edu.mt | info@euroamerican.edu.mt

Document Control

Document Title	Academic Integrity, Artificial Intelligence, Online Assessment and VLE Use Policy
Policy Number	EAI/2026/260401
Approval Authority	Senate
Implementation Authority	Rector and Head of Institution, Academic Committee and Quality Assurance Cell
Operational Responsibility	Dean of Quality Assurance, Controller of Exams, Programme Leaders, Module Leaders, Learning Design Support Office, IT Support and Data Protection Officer
Linked Existing Policies	IQA Manual, Privacy Policy, Data Protection Policy, Student Code of Conduct Policy, Student Grievances and Redressal Policy, Research Policy, Ethics Policy, Attendance and Participation Policy, Grading System Policy, Benchmarking Report Policy
External Regulatory Reference	MFHEA Regulations for Quality Assurance: Higher Education Online Learning, December 2025

Table of Contents

1.0 Purpose and Status of this Policy

This policy establishes the Institute specific controls for academic integrity, responsible use of artificial intelligence, online assessment integrity, VLE use, learning analytics and data protection in online and digitally supported learning.

It is deliberately drafted as a supplemental policy. It does not restate or replace the existing approved policies of the Euro American Institute. Where a matter is already governed by an approved policy, this policy provides only the additional online learning, AI, VLE or assessment integrity control required for implementation.

The purpose is to provide clear institutional evidence for online learning quality assurance, while avoiding duplication with existing policies on quality assurance, privacy, data protection, student conduct, grievances, research ethics, attendance, participation and grading.

This policy also supports the Institute's compliance with MFHEA requirements on online contact hours, including the required balance between synchronous and asynchronous contact hours. Programme and module documentation must specify the approved contact-hour structure and must evidence that contact hours are delivered, monitored and recorded through appropriate VLE, LMS, timetable, attendance and learning activity records.

This policy shall be read with the MFHEA Regulations for Quality Assurance: Higher Education Online Learning, December 2025, especially the requirements on assessment and integrity, technology resources, student support, AI literacy, human oversight, VLE records and ethical data practice.

2.0 Relationship with Existing Institutional Policies

This policy shall be interpreted together with the following approved institutional policies. The table explains the boundary between the existing policy and the additional provisions introduced here.

Existing Policy	Already Covered	Additional Scope of this Policy
Internal Quality Assurance Manual, EAI/2023/231212	Sets the institutional quality assurance framework, governance, programme design, student centred learning, assessment, student support, learning resources and research.	Adds operational controls for online assessment integrity, AI use, VLE evidence, learning analytics and MFHEA online learning compliance.
Privacy Policy, EAI/2024/241041	Public notice explaining collection, use, storage and protection of personal data for students, staff, website visitors and third parties.	Adds specific privacy notices and safeguards for VLE logs, online proctoring, AI tools, assessment evidence and learning analytics.
Data Protection Policy, EAI/2024/241032	Operational policy for handling student records, staff records, research data, IT systems and communications.	Adds data protection controls for digital assessment systems, AI enabled tools, identity verification, third party tools and audit logs.
Student Code of Conduct Policy, EAI/2024/241045	Defines student conduct, academic integrity expectations, misconduct, reporting, investigation, sanctions and confidentiality.	Adds specific rules for AI misuse, VLE credential misuse, digital impersonation, online assessment environment integrity and evidence handling.
Student Grievances and Redressal Policy, EAI/2024/241037	Provides the formal route for academic, administrative, disciplinary and online learning grievances.	Confirms that appeals and complaints about online assessment integrity decisions follow the approved grievance and appeal framework.
Research Policy, EAI/2023/231210 and Ethics Policy, EAI/2023/231209	Govern research integrity, ethical approval, plagiarism, data fabrication, informed consent, confidentiality and conflicts of interest.	Adds AI and digital tool safeguards for research writing, dissertation work, data analysis, authorship declarations and research supervision evidence.

Attendance and Participation Policy, EAI/2024/241043	Sets online attendance and participation expectations, engagement tracking, alerts, interventions and consequences.	Adds authentication, VLE log use, live session recording controls and digital attendance evidence for online learning compliance.
Grading System Policy, Policy #20230038	Sets grading principles and grade related rules.	Adds safeguards that grading, moderation and assessment decisions shall not be made solely by AI or automated systems.
Benchmarking Report Policy, EAI/2024/241050	Supports periodic benchmarking and improvement.	Adds a requirement to include online assessment practice, AI literacy, VLE use and academic integrity trends in future benchmarking where relevant.

3.0 Scope

This policy applies to all programmes, modules, awards, short courses, online learning activities and assessment activities delivered, managed, supported or assessed by Euro American Institute, including activities supported through approved student support service partners or online delivery partners.

It applies to:

- students, applicants where assessment or diagnostic testing is involved, alumni where academic records or verification are involved, and research students;
- academic staff, supervisors, tutors, markers, moderators, examiners and external experts;
- administrative staff, quality assurance staff, examinations staff, IT support staff and student support staff;
- approved digital systems, VLE or LMS platforms, live teaching platforms, online assessment tools, plagiarism checking tools, AI or GenAI tools and learning analytics systems;
- academic work submitted for credit, progression, award, research supervision, dissertation, thesis, viva, presentation, quiz, online examination, project, portfolio or any other assessment purpose.

The policy does not create a separate disciplinary code, separate grievance mechanism or separate data protection policy. Those matters remain governed by the relevant approved policies listed in section 2.0.

4.0 Definitions Used in this Policy

Definitions are used only where necessary to support implementation. Where MFHEA or institutional policy definitions already exist, those definitions shall prevail.

Term	Meaning in this Policy
Academic integrity	Honest, responsible and ethical conduct in learning, assessment, research, authorship, collaboration, citation, data use and communication.
Artificial intelligence or AI	Digital systems that can generate, classify, analyse, summarise, predict, recommend or produce content or decisions using computational models.
Generative AI or GenAI	AI tools that generate text, code, images, audio, video, data analysis, summaries, translations or other content based on prompts or uploaded material.
VLE or LMS	The approved virtual learning environment or learning management system used for teaching, learning, assessment, communication, attendance records, student engagement tracking and academic evidence.
Online assessment integrity	The set of controls that provide reasonable confidence that online assessment evidence is authentic, secure, fair, attributable to the student and aligned with learning outcomes.
Learning analytics	The collection and interpretation of VLE, LMS or digital learning data for student support, engagement monitoring, quality assurance, retention and programme improvement.
Proctoring	A controlled process used where necessary to verify identity and protect the integrity of a test, online examination or controlled assessment environment.

5.0 Policy Principles

- Human academic judgement shall remain central. AI tools, similarity tools, proctoring tools and learning analytics may support academic judgement, but shall not replace it.
- Assessment shall be designed first for learning outcomes, authenticity and fairness. Technology shall support assessment design and shall not dictate it.
- Students shall receive clear instructions on permitted AI use, collaboration, citation, identity verification, submission format and assessment conditions before assessment takes place.
- Online assessment evidence shall be capable of verification through appropriate combinations of VLE logs, similarity reports, version history, oral verification, live presentation, supervision records, proctoring records or examiner judgement.
- Personal data shall be processed lawfully, transparently, fairly, securely and only to the extent necessary for academic, administrative, quality assurance, regulatory or student support purposes.
- The Institute shall avoid duplicating policy mechanisms. Student misconduct, grievances, appeals, research ethics and data protection matters shall be routed through the approved institutional policies already in force.
- Students and staff shall be supported through induction, training, guidance and accessible communication, rather than relying only on punitive measures.

6.0 Governance, Roles and Responsibilities

Role or Unit	Responsibility under this Policy
Senate	Approves this policy and any substantive amendments.
Rector and Head of Institution	Ensures institutional implementation and confirms that the policy is embedded into programme delivery, assessment and reporting.
Academic Committee	Reviews academic implementation, programme level assessment design, academic integrity trends and staff guidance.
Quality Assurance Cell	Monitors implementation, maintains evidence, coordinates review and includes relevant findings in internal quality assurance reporting.
Dean of Quality Assurance	Coordinates the online learning compliance evidence required for MFHEA, including assessment integrity and VLE related quality controls.
Controller of Exams	Ensures that online assessments, controlled assessments, identity checks, assessment records, moderation evidence and grade related evidence are managed according to approved procedures.
Learning Design Support Office	The Learning Design Support Office shall serve as the Institute's educational and instructional design support unit for online and digitally supported learning. Separate from the Data Protection Officer and quality assurance function, it works collaboratively with both to support online course design, VLE structure, digital learning activities, assessment design, accessibility, AI-aware learning, and staff guidance on online pedagogy.
Data Protection Officer	Reviews data protection implications of VLE use, online proctoring, AI tools, learning analytics, third party tools and retention arrangements.
Programme Leaders and Module Leaders	Communicate assessment rules, AI permissions, academic integrity requirements, rubrics, submission instructions and verification procedures to students.
Academic Staff and Supervisors	Provide guidance, monitor submissions, apply academic judgement, record concerns and use approved systems responsibly.

Students	Use their own credentials, submit authentic work, follow assessment instructions, declare AI use where required and comply with academic integrity rules.
IT Support	Maintains secure access, system logs, backups, access controls, user support and system availability for approved platforms.

7.0 Academic Integrity in Online and Digital Learning

The Student Code of Conduct Policy remains the governing policy for misconduct and sanctions. This section adds the online and digital academic integrity controls required for implementation.

7.1 Core Academic Integrity Expectations

- All assessed work must be the student's own work except where collaboration is expressly permitted.
- Sources, data, quotations, paraphrased material, images, code, tables, AI generated assistance and external support must be acknowledged according to the assessment instructions and approved referencing style.
- Students must not impersonate another student, share login credentials, permit another person to complete assessment, use contract cheating services or submit work created substantially by another person or tool as their own.
- Students must retain drafts, notes, references, version history, data files, supervision records and AI use records where these may be required to verify authorship or research integrity.
- Academic staff may require oral verification, viva style discussion, presentation, draft review or additional evidence where there is a reasonable concern about authorship, academic integrity or AI misuse.

7.2 Minimum Integrity Controls

At minimum, the following controls shall be applied where relevant to the assessment type:

- written assignments, projects, research papers and dissertations shall be submitted through the approved VLE submission route unless an exception is approved;
- similarity checking shall be used for written academic work where appropriate and available;
- AI detection indicators may be considered only as supporting information and not as sole evidence of misconduct;
- assessment briefs shall state whether AI use is prohibited, permitted with declaration, required as part of learning, or limited to specific tasks;
- rubrics shall state how originality, analysis, citation, methodology, data use, presentation and reflection are assessed;
- where authorship is uncertain, staff shall use human academic review supported by draft evidence, oral verification, student explanation, VLE records and supervisor records.

8.0 Artificial Intelligence and Generative AI Use

The Institute recognises that AI and GenAI can support learning, teaching, instructional design, research preparation, accessibility and administrative efficiency. At the same time, AI use must be transparent, ethical, fair, lawful and consistent with the learning outcomes of each programme and module.

8.1 AI Permission Categories

Category	Requirement
Category A: AI use prohibited	AI tools must not be used for the assessment or task. Students must complete the work independently except for ordinary spell checking and formatting tools, unless otherwise stated.
Category B: AI use permitted with declaration	AI may be used for limited support such as brainstorming, language refinement, outlining, coding assistance, translation support or data exploration, but the student must declare the nature and extent of use.
Category C: AI use required or assessed	AI use forms part of the learning activity or assessment. Students must demonstrate critical evaluation, verification, ethical awareness and appropriate documentation of AI output.
Category D: Staff supported AI use	Academic staff may use AI to support instructional design, examples, formative feedback preparation or administrative drafting, but must verify accuracy and protect data.

8.2 Student Rules for AI Use

- Students must follow the AI permission category stated in the module guide, assessment brief or VLE assessment instructions.
- Where AI is used, students must keep a record of tool name, date of use, purpose of use, prompt summary and the way in which the output was verified or adapted.
- Students must not upload personal data, confidential student information, unpublished institutional material, research participant data or assessment material into public AI tools unless the tool and purpose have been approved.
- Students remain fully responsible for the accuracy, originality, citations, interpretation, ethical compliance and academic quality of submitted work.
- Undeclared or prohibited AI use may be treated as academic misconduct under the Student Code of Conduct Policy.

8.3 Staff Rules for AI Use

- Academic staff may use AI to support teaching preparation, examples, activity design and formative guidance only where academic judgement remains with the staff member.
- AI shall not be used to make final academic decisions, progression decisions, misconduct decisions, admissions decisions or award decisions without human review and accountable approval.
- Staff must not enter student personal data, confidential assessment information, research participant data or unpublished institutional information into public AI tools unless approved by the responsible authority and reviewed for data protection compliance.

- Where AI is used in assessment design or student facing learning activity, the module documentation should explain the purpose, limits and expectations clearly.

9.0 Online Assessment Integrity

This section supplements, but does not replace, the Grading System Policy, Student Code of Conduct Policy, Student Grievances and Redressal Policy and relevant programme assessment regulations.

9.1 Assessment Design Controls

- Online assessments shall be aligned with programme learning outcomes and module learning outcomes.
- Where possible, assessment design should use authentic, applied, reflective, oral, project based, portfolio based, research based or performance based methods that reduce the risk of impersonation and unsupported AI generation.
- High stakes timed online examinations shall only be used where the Institute has appropriate arrangements for identity verification, environment integrity and secure assessment administration.
- If appropriate online proctoring or equivalent integrity arrangements are not available for a high stakes timed online examination, the assessment shall be redesigned or delivered through another approved controlled format.
- Assessment briefs shall communicate permissible resources, collaboration rules, AI permissions, submission route, late submission rules, rubric, moderation arrangements and academic integrity checks.

9.2 Identity Verification

- Each student shall use their own approved institutional credentials for VLE access and assessment submission.
- Live presentations, viva style assessments, oral verification, supervision meetings and controlled assessments may require visual identity confirmation by the academic staff member or authorised assessment staff member.
- Where additional identity evidence is required, only the minimum necessary information shall be requested and processed in accordance with the Privacy Policy and Data Protection Policy.
- Credential sharing, impersonation or allowing another person to access an assessment account is serious academic misconduct.

9.3 Proctoring and Controlled Assessment

- Proctoring shall be used only where proportionate to the nature, stakes and risk of the assessment.
- Proctoring may include live invigilation, recorded invigilation, locked assessment windows, screen or camera checks, secure browser features, identity checks or other approved measures.
- Students shall be informed in advance about the type of proctoring, data collected, purpose, retention, access, technical requirements and support arrangements.
- Formative activities used only for learning checks do not normally require proctoring.
- Any proctoring provider shall be reviewed for data protection, security, accessibility, reliability and service support before adoption.

9.4 Evidence and Record Keeping

- Assessment evidence may include submitted files, timestamps, VLE logs, similarity reports, marker comments, moderation records, oral verification notes, presentation records, proctoring reports, version history and student declarations.
- Evidence shall be retained according to approved institutional retention rules and only accessed by authorised personnel.
- Where an academic integrity concern is raised, evidence shall be handled confidentially and routed through approved procedures.

10.0 VLE, LMS and Digital Learning Use

The VLE or LMS is the official academic environment for online learning, student engagement, assessment submission, tutor support, learning resources and evidence of participation. This section supplements the Attendance and Participation Policy and Student Code of Conduct Policy.

10.1 Access and Authentication

- Students and staff shall access the VLE using approved credentials only.
- Users must not share passwords, allow another person to use their account or access another user account without authorisation.
- The Institute may use VLE logs to support attendance, participation, student support, academic integrity, quality assurance, security and regulatory evidence.
- Access rights shall be role based and removed or changed when a user role changes or ends.

10.2 Learning Resources and Intellectual Property

- Learning resources shall be uploaded, shared and accessed in accordance with intellectual property rights and the relevant institutional policies.
- Students must not copy, distribute, record, upload, sell or publicly share teaching materials, live sessions, recordings, peer work or assessment materials without approval.
- Staff shall use copyright compliant materials, open educational resources or institutionally approved resources wherever possible.

10.3 Recordings and Live Sessions

- Live teaching sessions may be recorded where there is a legitimate academic, accessibility, quality assurance or student support purpose.
- Students and staff shall be informed when a session is recorded and how the recording may be accessed.
- Recordings shall be made available only through approved institutional channels and normally only to the relevant cohort and authorised staff.
- Sensitive personal issues, private student matters and disciplinary discussions should not be recorded unless required and approved for a clear lawful purpose.

10.4 Accessibility and Technical Support

- The Institute shall aim to ensure that digital resources are accessible on commonly available devices and do not require students to purchase high end hardware unless clearly justified by programme requirements.
- Students shall be given information on how to access VLE support, technical support, academic support and assessment support.
- Accessibility needs shall be considered in online learning design and assessment arrangements in accordance with the relevant student support and equality policies.

10.5 Synchronous and Asynchronous Contact-Hour Evidence

- The Institute shall ensure that online programmes comply with MFHEA requirements on contact hours, including the requirement that contact hours represent at least 20% of total learning hours.
- For programmes carrying ECTS, each ECTS shall include at least five contact hours, of which a minimum of four hours must be delivered synchronously and up to one hour may be delivered asynchronously, unless otherwise approved or required by MFHEA.
- Synchronous contact hours may include live online lectures, seminars, tutorials, workshops, supervision meetings, virtual office hours, real-time academic feedback, presentations, research clinics and online collaborative sessions involving the virtual presence of an educator.
- Structured asynchronous contact hours may include interactive recorded lectures requiring student responses and educator feedback, educator-moderated online discussions, interactive online exercises under educator supervision, recorded student presentations requiring educator feedback, and other supervised asynchronous activities that involve meaningful interaction between students and educators.
- Non-contact activities, including independent reading, self-directed study, non-interactive recorded lectures, unsupervised work, assessment preparation and time spent completing assessment tasks, shall not be counted as contact hours unless they meet the applicable MFHEA definition of contact learning.
- Programme leaders and module leaders shall ensure that module guides, timetables and VLE areas identify the intended synchronous and asynchronous contact-hour allocation. Attendance records, VLE logs, forum records, activity completion data, supervision records and tutor feedback records shall be retained as evidence of delivery, learner engagement and regulatory compliance.

10.6 Approved Digital Tools and Technology Review

- All digital tools used for teaching, learning, assessment, proctoring, similarity checking, learning analytics, AI-supported activity, student communication or VLE delivery shall be approved by the Institute before implementation.
- Before adopting or materially changing a digital tool, the relevant responsible office shall consider:
    - pedagogical suitability;
    - alignment with programme and module learning outcomes;
    - accessibility and reasonable adjustment requirements;
    - data protection and privacy implications;
    - information security and access controls;
    - reliability, technical support and continuity arrangements;
    - compatibility with the VLE/LMS and institutional systems;
    - staff and student training requirements;

  - record-keeping and audit requirements;
  - contractual safeguards where third-party providers are involved.
- The Data Protection Officer shall be consulted where the tool involves personal data, identity verification, proctoring, learning analytics, AI processing, recording, third-party storage or any higher-risk data processing activity.
- The Learning Design Support Office, IT Support and Quality Assurance Cell shall keep appropriate records of approved tools, implementation decisions, technical support arrangements and review outcomes.

11.0 Data Privacy and Digital Records Controls for VLE, AI and Online Assessment

This section supplements the Privacy Policy and Data Protection Policy. It does not replace the rights, principles, legal bases, retention obligations or breach procedures already contained in those policies.

11.1 Specific Data Protection Controls

- VLE, LMS, assessment, proctoring, similarity checking and learning analytics tools shall collect only the data necessary for academic, student support, quality assurance, regulatory, security or legal purposes.
- Students shall be informed about the use of VLE logs, assessment logs, identity verification data, proctoring data, similarity reports and learning analytics where relevant.
- Access to academic integrity evidence, assessment records, proctoring records and learning analytics shall be restricted to authorised staff with a legitimate role.
- Third party digital tools shall be reviewed for data protection, information security, service reliability and contractual safeguards before being adopted for institutional use.
- Where a digital tool introduces significant privacy risk, the Data Protection Officer shall be consulted and a data protection impact assessment or equivalent review shall be considered.
- Personal data shall not be uploaded to public AI tools unless the tool, purpose and legal basis are approved and appropriate safeguards are in place.
- No student shall be subject to a final academic, disciplinary, progression or award decision based solely on automated processing or AI generated judgement.

11.2 Retention and Disposal

- Assessment submissions and academic records shall be retained according to approved institutional academic record retention requirements.
- Technical logs, proctoring records and analytics records shall be retained only for the period necessary for academic administration, appeals, complaints, quality assurance, security and regulatory evidence.
- Where evidence is connected to an appeal, complaint, investigation, legal matter or regulatory matter, it may be retained until the matter is concluded and any applicable limitation period has expired.
- Secure deletion or access removal shall be applied when records are no longer required.

12.0 Student and Staff Induction

The Institute shall provide appropriate guidance to students and staff before or during programme delivery. This guidance may be delivered through the VLE, induction sessions, module guides, assessment briefs, staff briefings or student handbooks.

12.1 Student Induction shall Cover

- VLE access, credentials, communication channels and support routes;
- attendance, participation and engagement expectations;
- assessment submission routes, file formats, deadlines and rubrics;
- academic integrity, plagiarism, citation, paraphrasing and referencing;
- AI use categories, AI declaration and prohibited use;
- identity verification, oral verification, proctoring and online assessment rules where relevant;
- data protection, privacy notices and responsible digital conduct.

12.2 Staff Induction shall Cover

- VLE course setup, assessment release, submission management and feedback recording;
- online assessment design, rubrics, moderation evidence and academic integrity checks;
- responsible AI use in teaching, learning and assessment;
- human review of AI indicators and similarity reports;
- student support escalation and referral routes;
- data protection duties and approved digital tool use.

The policy, student-facing guidance, AI declaration requirements, online assessment rules, VLE instructions, technical support routes, academic integrity expectations and relevant privacy information shall be made available through the VLE, student handbook, module guides, assessment briefs and programme induction. Students shall be informed before assessment of the permitted use of AI, collaboration rules, citation expectations, identity verification arrangements, proctoring arrangements where applicable, similarity checking, submission requirements, appeal routes and relevant data-processing information.

13.0 Monitoring, Evidence and Continuous Improvement

The Quality Assurance Cell shall monitor implementation through existing quality assurance mechanisms. This policy adds the following online learning and assessment integrity evidence areas.

- sample module guides showing AI permissions, assessment instructions and online assessment controls;
- sample VLE pages showing student access to policy information, assessment briefs, rubrics and support information;
- records of student induction and staff briefing on academic integrity, AI, VLE use and online assessment;
- sample similarity reports, moderation records, oral verification notes and assessment evidence where applicable;
- records of student complaints, appeals or technical issues related to online assessment, routed through approved procedures;
- periodic review of AI, academic integrity, VLE engagement and online assessment risks;
- evidence that third party digital tools have been reviewed for privacy, security and suitability before use.

Findings shall be reported through existing quality assurance reporting and programme review channels. The policy shall be updated when MFHEA requirements, GDPR guidance, EU AI related obligations, technology practice or institutional operations materially change.

The Quality Assurance Cell shall include online learning and assessment-integrity evidence in programme monitoring and periodic review. Evidence may include VLE activity data, attendance records, engagement analytics, assessment submission data, similarity checking trends, academic misconduct trends, AI-use declarations, student feedback, staff feedback, technical support issues, accessibility concerns, proctoring or identity-verification issues, and outcomes of moderation or assessment review.

Where learning analytics or VLE data indicate that a student may be at risk of disengagement, non-progression or assessment difficulty, the matter shall be referred through the approved student support and academic monitoring processes.

14.0 Academic Misconduct Referral and Appeal Routes

This policy does not create a separate disciplinary route. It provides the online learning and AI related evidence rules that support the approved Student Code of Conduct Policy and Student Grievances and Redressal Policy.

14.1 Referral Process

- Where academic staff identify a concern about plagiarism, AI misuse, collusion, impersonation, contract cheating, assessment environment breach or VLE credential misuse, the concern shall be documented with available evidence.
- The module leader or programme leader shall undertake an initial academic review to determine whether the matter can be resolved as poor academic practice, needs student guidance or should be referred as suspected misconduct.
- Where suspected misconduct is referred, the Student Code of Conduct Policy shall govern investigation, communication, decision and sanctions.
- Students shall be given a fair opportunity to respond to concerns and provide evidence such as drafts, notes, source records, AI use records, version history or oral explanation.
- Where a student wishes to appeal or complain about process, outcome, assessment conditions or alleged unfair treatment, the Student Grievances and Redressal Policy shall apply.

14.2 Evidence Limits

- A similarity percentage alone shall not automatically establish plagiarism.
- An AI detection score alone shall not establish AI misconduct.
- A VLE log anomaly alone shall not establish misconduct without reasonable contextual review.
- Academic judgement shall consider the assessment instructions, student level, draft evidence, citation practice, oral verification and all available circumstances.

15.0 Review and Version Control

This policy shall be reviewed annually by the Quality Assurance Cell in consultation with the Academic Committee, Controller of Exams, Data Protection Officer, Learning Design Support Office, student representatives and relevant academic staff.

Earlier review shall be triggered by any of the following:

- MFHEA regulatory change or evaluator recommendation;
- change in institutional VLE, LMS, assessment system, proctoring system or AI tool;
- significant academic integrity incident or trend;
- data protection incident or material privacy risk;
- new legal or regulatory requirements relating to AI, data protection, online assessment or digital learning.

Appendix A: AI Use Declaration

This declaration may be embedded into assessment submission forms, VLE submission boxes or assessment cover sheets where AI use is permitted or where the module leader requires a declaration.

Student Name	
Student ID	
Programme and Module	
Assessment Title	
AI Tool Used	State tool name or write 'Not Used'.
Purpose of Use	For example brainstorming, language refinement, data exploration, coding support, translation support or no use
Extent of Use	Briefly describe what was AI-supported and what was independently completed
Verification	Explain how accuracy, citation, originality and interpretation were checked
Student Declaration	I confirm that this submission complies with the assessment instructions and the Academic Integrity, AI, Online Assessment and VLE Use Policy.
Date	

Appendix B: Online Assessment Integrity Checklist

1. [ ] Learning outcomes are clearly aligned with the assessment task.
2. [ ] Assessment type and weighting are stated in the module guide or assessment brief.
3. [ ] AI permission category is stated clearly.
4. [ ] Collaboration rules and citation requirements are stated clearly.
5. [ ] Submission route and deadline are stated clearly.
6. [ ] Rubric is available to students before submission.
7. [ ] Identity verification method is appropriate to the assessment risk.
8. [ ] Proctoring or controlled assessment arrangements are confirmed where required.
9. [ ] Similarity checking is enabled where appropriate.
10. [ ] Oral verification or viva style confirmation is available where authorship is uncertain.
11. [ ] Data protection information is provided for proctoring, third party tools or unusual data processing.
12. [ ] Accessibility and reasonable adjustment needs have been considered.
13. [ ] Moderation and record keeping arrangements are confirmed.
14. [ ] Appeal and grievance route is available to students.

Appendix C: MFHEA and Existing Policy Mapping

MFHEA Area	Requirement Addressed	Where Addressed
MFHEA Domain 1: Leadership and Management	AI is included in institutional strategy, policy and budget consideration.	Sections 2.0, 6.0, 8.0 and 13.0
MFHEA Domain 2: Staffing Profile and Professional Development	Staff induction and AI guidance are required.	Sections 6.0 and 12.0
MFHEA Domain 3: Programme Learning Outcomes	Ethical and responsible AI use may be embedded in outcomes where relevant.	Sections 8.0 and 9.1
MFHEA Domain 4: Curriculum Design	Online learning design, student interaction and AI aware learning are supported.	Sections 8.0, 9.0, 10.0 and 12.0
MFHEA Domain 5: Assessment and Integrity	Online assessment policies, proctoring, plagiarism, GenAI rules, human review and appeals are addressed.	Sections 7.0, 8.0, 9.0 and 14.0
MFHEA Domain 6: Programme Review and Improvement	Learning analytics and academic integrity trends support review.	Section 13.0
MFHEA Domain 7: Technology Resources	VLE use, access control, recordings, security, data protection and AI tool review are addressed.	Sections 10.0 and 11.0
MFHEA Domain 8: Student Information, Experience and Support	Student induction, support routes, VLE guidance and academic writing guidance are addressed.	Sections 10.4, 12.0 and 14.0

Appendix D: References and Controlled Documents

- Euro American Institute Internal Quality Assurance Manual, Policy # EAI/2023/231212.
- Euro American Institute Privacy Policy, Policy # EAI/2024/241041.
- Euro American Institute Data Protection Policy, Policy # EAI/2024/241032.
- Euro American Institute Student Code of Conduct Policy, Policy # EAI/2024/241045.
- Euro American Institute Student Grievances and Redressal Policy, Policy # EAI/2024/241037.
- Euro American Institute Research Policy, Policy # EAI/2023/231210.
- Euro American Institute Ethics Policy, Policy # EAI/2023/231209.
- Euro American Institute Attendance and Participation Policy, Policy # EAI/2024/241043.
- Euro American Institute Grading System Policy, Policy #20230038.
- MFHEA Regulations for Quality Assurance: Higher Education Online Learning, December 2025.
- General Data Protection Regulation and applicable Maltese data protection legislation.