

# Generative AI in Higher Education Teaching & Learning

## Procurement & Vendor Governance

### Contributors

James O'Sullivan  
Colin Lowry  
Ross Woods  
Tim Conlon

HEA Generative AI Policy Framework

<https://hub.teachingandlearning.ie/genai/policy-framework>

HEA Generative AI Resource Portal

<https://hub.teachingandlearning.ie/genai/>

Version 1.0, December 2025

Higher Education Authority, Dublin

DOI: 10.82110/wyh1-vs46

How to cite:

O'Sullivan, James, Colin Lowry, Ross Woods & Tim Conlon. *Generative AI in Higher Education Teaching & Learning: Procurement & Vendor Governance*. Dublin: Higher Education Authority, 2025.

DOI: 10.82110/wyh1-vs46.

This document, and all original content contained within, is licensed under the [Creative Commons Attribution-ShareAlike 4.0 International Public License \(CC BY-SA 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/).



## Purpose and scope

Higher education institutions should adopt generative AI systems and gen AI-enabled tools only where they demonstrably advance educational aims and can be governed in a manner consistent with public value and institutional commitments to academic integrity, transparency, privacy, equity, accessibility, and sustainability.

It is recognised that generative AI systems, by their very design, can sit in tension with several of these commitments, particularly where probabilistic outputs, limited model transparency, opaque training data provenance, and vendor-controlled update cycles constrain meaningful explainability or sustainability assurance.

Institutions should proceed on the presumption that such tensions should be surfaced, and where compromises are proposed, they must be explicitly identified, their necessity and proportionality justified, and the residual risks and mitigations recorded in a form suitable for institutional scrutiny and public accountability.

This policy applies to any generative AI system that generates or transforms content, including text, code, images, audio, video, or synthetic data, and is used, supported, funded, licensed, or endorsed by the institution for teaching and learning purposes. It includes tools used in:

1. Learning activities, tutoring, study support, and skills development;
2. Staff workflows that shape learning and teaching (learning design, marking support, feedback drafting, rubric development, content creation);
3. Assessment design and delivery, including formative and summative assessment, academic integrity processes, and feedback mechanisms;
4. Student support and engagement functions closely coupled to learning (advising, writing support, induction resources), where gen AI outputs are presented as guidance.

It also applies to pilots, trials, 'freemium' offerings, embedded gen AI features inside platforms (VLEs, productivity suites, library systems), and any integration that processes institutional or student data.

## Roles and responsibilities

Policy Owner (Registrar or equivalent)	Approves adoption; confirms and records risk acceptance; ensures transparency obligations are met.
Academic governance/Quality	Assures alignment with programme standards, assessment regulations, academic integrity policy, and external quality expectations.
Centre for Teaching and Learning (CTL)	Evaluates pedagogic fit, supports implementation, and coordinates staff development and guidance for practice.
Procurement	Ensures compliant sourcing and that minimum evidence requirements are met; maintains procurement file completeness.
Data Protection Officer (DPO)	Oversees DPIA completion and review; advises on lawful basis, fairness, transparency, and student rights.
IT Security	Assesses security posture, access control, logging, and incident readiness; assures integration security.
Accessibility Lead	Verifies conformance and remediation commitments; assures accessible user journeys.
EDI function	Assesses inclusion impacts (including language performance and differential error patterns).
Students' Union and student representatives	Consulted for material changes to learning conditions, assessment expectations, or data processing.



## Procurement processes

### Before market engagement: defining the teaching and learning need

Before any market engagement, including demonstrations where institutional data or teaching materials may be shared, the proposing unit should complete a teaching and learning ‘public value case’ that records:

1. The educational purpose, stated as a problem definition linked to learning outcomes or teaching quality aims, with expected benefits and a plan for evaluating those benefits;
2. Consideration of non-gen AI alternatives (including pedagogic redesign, staffing, peer learning supports, or existing digital tools), with reasons for preferring gen AI;
3. The institution’s risk appetite for the proposed use, including an explicit statement of what will not be accepted (for example, automated grading without robust oversight);
4. Stakeholder identification from the outset, including the Policy Owner, Procurement, DPO, IT Security, Accessibility, Quality, CTL, EDI, and student representation;
5. High-level EU AI Act scoping to classify the use case and identify any high-risk triggers, particularly those that affect assessment, progression, or student support decisions.

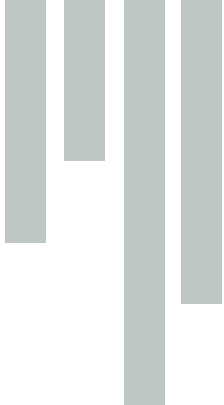
No procurement, pilot, or deployment may proceed until these artefacts are complete and accepted by Procurement and the Policy Owner.

### Minimum evidence to request from vendors

Vendors should provide evidence sufficient to evaluate educational safety, governance feasibility, and compliance. As a minimum, institutions should request and retain:

### Security and operational assurance

1. A recognised security posture, including controls relevant to identity and access management, encryption, vulnerability management, and secure development practices;
2. A defined breach-response process with timelines, escalation routes, and clear roles;

- 
3. Version control and change management practices, including release notes for model and system updates;
  4. Allowance for independent verification (audit reports, third-party assurance, penetration testing summaries, or equivalent).

## Data governance and privacy

1. A data governance map showing all data flows, storage locations, hosting arrangements, sub-processors, retention and deletion procedures, data minimisation measures, and cross-border transfer assessments;
2. Clarity on whether prompts, outputs, telemetry, and user interaction logs are stored, for how long, and for what purposes;
3. Explicit statements on whether institutional or student data are used for model training, fine-tuning, evaluation, or product improvement, and under what controls.

## Model and output risk documentation

1. Full system documentation specifying purpose, expected inputs and outputs, update cadence, known limitations, and failure modes relevant to teaching and learning;
2. Documented risks and mitigations for hallucination, prompt injection, data leakage through prompts, and harmful or inappropriate output generation;
3. Evidence of robustness measures, including content filtering, safety tuning, guardrails, and monitoring for misuse patterns.

## Bias, equity, and language performance

1. Evidence of bias and equity management, including what is known about training data provenance and representativeness, documented limitations, and evaluation protocols;
2. Evidence of performance testing in Irish and other relevant minority languages, with disclosure of known degradation patterns and proposed mitigations.



## Accessibility

1. Accessibility conformance evidence against recognised international standards, with a time-bound remediation plan for deficiencies and named accountability.

## Sustainability

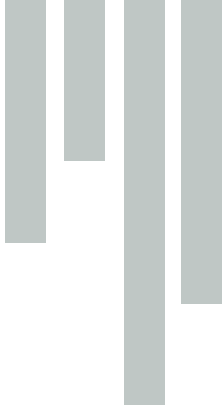
1. Sustainability disclosures, proportionate to scale and deployment model, describing energy footprint indicators, data centre sourcing, and efficiency measures.

Where evidence is incomplete, the default presumption is non-adoption unless a documented exception is approved with compensating controls.

## Legal and contractual safeguards

Contracts and licences must include enforceable protections appropriate to generative AI risks in education:

1. Institutional and student data must remain the property of the institution or the student (as applicable) and must not be used to train or fine-tune external models without explicit, granular consent that is freely given and revocable to the extent permitted by law;
2. Purpose limitation should be explicit and should cover prompts, outputs, logs, and metadata, with maximum retention periods and technical enforcement where possible;
3. Secure deletion must be verifiable at contract end, including deletion of stored prompts, outputs, and logs where these contain personal data or confidential academic materials;
4. The institution should retain audit and assurance rights proportionate to risk, including the right to receive timely notification of significant changes (model updates, sub-processor changes, hosting location changes, pricing/terms changes that affect governance) and access to documentation in clear, non-technical language;
5. Liability and indemnity should allocate responsibility proportionately for non-compliance, security failures, and material misrepresentation of tool capabilities or limitations;

- 
6. The institution must retain the unilateral right to suspend or terminate where material risk emerges or terms change, with a continuity or transition plan that protects teaching delivery and students' ability to complete assessment fairly.

## **Regulatory compliance pack for teaching and learning deployments**

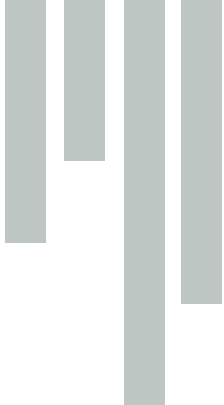
For each approved generative AI tool, a compliance pack must be assembled, maintained, and reviewed:

1. A DPIA must be completed where required, and in any case where gen AI is used at scale, processes student personal data, or influences assessment conditions. The DPIA must address fairness, explainability, accessibility, cumulative risk, and student rights, and be reviewed annually;
2. EU AI Act control requirements must be mapped where applicable, including human oversight, logging, robustness and accuracy testing, and an explicit statement of oversight competence (who can intervene, how they are trained, and what authority they hold);
3. Plain-language transparency notices should be available at point of use and on the institutional transparency page, including clear statements about limitations, typical failure modes, and appropriate reliance;
4. Accessibility verification should be attached to the procurement file, or a time-bound remediation plan with an assigned owner must be documented.

## **Academic integrity and assessment safeguards**

Because gen AI directly affects authorship, evidence of learning, and assessment validity, the following requirements should be applied:

1. Every deployment should specify its relationship to assessment: whether gen AI use is permitted, required, conditionally permitted, or prohibited, and how this aligns with learning outcomes;
2. Where generative AI tools are permitted in assessed work, assessment design should include mechanisms that preserve valid measurement of the intended competencies. Where this cannot be achieved, gen AI use must be restricted or the assessment redesigned;

- 
3. Where external generative AI tools are permitted, students must be required to declare use in a clear, non-punitive manner that supports transparency rather than surveillance, unless prohibited by assessment rules;
  4. Students must have access to non-gen AI pathways where gen AI use would otherwise be effectively compulsory, including where disability, language, conscientious objection, or privacy concerns are implicated;
  5. Any use of generative AI to support marking, feedback drafting, or academic integrity processes must include human review responsibilities and clear limits on automation, with documentation of how judgement is exercised.

## Equity, language, and inclusion checks

To avoid unequal learning conditions and exclusionary effects:

1. Core teaching and learning uses must be supported through institution-licensed access, so that students and staff are not forced into personal subscriptions or unequal tooling;
2. Tools should be evaluated for performance in Irish and other relevant minority languages, including disclosure of performance gaps and the provision of compensatory supports or alternatives where needed;
3. Differential error patterns affecting protected or marginalised groups must be considered during pilots and monitored in operation, with a documented plan for response and remediation.

## Governance and records

The institution should maintain auditable governance for each approved generative AI tool:

1. Each tool should have an entry in the institutional Tool Register, recording evaluation criteria, methods, results, limitations, adoption rationale, training requirements, and monitoring plans. A public version should be maintained, with appropriate redactions for security;
2. Named owners should be assigned: a service owner for operational delivery; an accountable executive (Registrar or equivalent); and a maintenance owner responsible for monitoring, vendor liaison, and termly change verification;
3. Documentation (register entries, DPIAs, contracts, declarations, logs, training records, incident reports) should be retained in line with institutional schedules and be available for





internal audit and external scrutiny where appropriate.

## Implementation and change management

Implementation should embed oversight, competence, and clear practice expectations:

1. Human oversight mechanisms should be designed into workflows, specifying review responsibilities, review timing, and escalation paths;
2. Module and programme documentation should state the permitted use of generative AI, expected citation or acknowledgement practices, and boundaries around substituting gen AI outputs for student work;
3. Staff and student training must be scheduled and tracked, with measurable coverage indicators and refresher expectations where tools or policies change;
4. Institutional transparency obligations should be met via publication of Tool Register updates, approved exceptions, material incidents in appropriately anonymised form, and aggregate training coverage;
5. Change logs and vendor update notes must be reviewed before each academic term, with support responsiveness and uptime performance recorded.

## Monitoring, incidents, and review

Because generative AI tool performance can shift with updates and drift, ongoing oversight is required:

1. Continuous monitoring should be proportionate to risk and must address accuracy, bias, drift, safety failures, and outages, with defined triggers for re-evaluation;
2. Incident and harm-response processes should align to institutional procedures, including drills, severity triage, containment, and timely DPO notification where data protection issues arise;
3. Annual re-evaluation is mandatory for each approved tool, covering compliance status, incident history, model changes, emerging risks, and educational impact evidence. Where risks become unacceptable, decommissioning must occur with continuity plans enacted.



## Exceptions

Exceptions should be approved only where necessity is documented, compensating controls are credible, and approvals are recorded. Exceptions should be time-limited and entered into the Tool Register with review dates. Where exceptions affect assessment conditions, Quality and the Policy Owner should sign off, with student and staff communication requirements met.

## Enforcement

Non-compliant deployments should be suspended pending review. Where generative AI use materially affects assessment validity, student rights, or data protection compliance, the institution should prioritise immediate risk containment, clear communication to affected cohorts, and governance remediation.

## Review and revision

Procurement policies should be regularly reviewed, and additionally following material incidents, significant vendor changes, or regulatory updates. Revisions should proceed through formal governance routes and be communicated via the mechanism for institutional transparency.