HEA | An tÚdarás um Ard-Oideachas
The Higher Education Authority

# Generative AI in Higher Education Teaching & Learning

## Roles & Responsibilities: IT & Data Protection

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
DOI: 10.82110/tb5d-8z75
Higher Education Authority, Dublin

How to cite:
O'Sullivan, James, Colin Lowry, Ross Woods & Tim Conlon. *Generative AI in Higher Education Teaching & Learning: Roles & Responsibilities (IT & Data Protection)*. Dublin: Higher Education Authority, 2025. DOI: 10.82110/tb5d-8z75.

IT services and data protection officers occupy a fundamental role in the institutional governance of generative AI. Together, they provide the technical, legal, and procedural safeguards that enable innovation while ensuring that enthusiasm for AI adoption does not exceed the university's capacity to manage risk, comply with regulation, or protect staff and student data. Their work underpins trust in institutional systems and is essential to sustaining lawful and responsible AI use across teaching and learning.

IT services are responsible for the deployment and maintenance of secure technical infrastructure for generative AI, which includes the provision of institutionally approved AI tools that are integrated through secure authentication mechanisms such as single sign-on, ensuring that usage can be monitored, supported, and, where necessary, restricted. Shadow use of unvetted third-party tools poses significant risks to data security and institutional compliance; IT services therefore have a duty to offer viable, supported alternatives that reduce the incentive for unsanctioned use.

Security considerations extend beyond basic access control and IT services must actively assess and mitigate risks associated with prompt injection, data leakage, model misuse, and adversarial exploitation. This includes monitoring system usage for anomalous patterns, maintaining appropriate logging and audit capabilities, and ensuring that institutional networks and endpoints are resilient to emerging attack vectors associated with AI-enabled systems. Generative AI should be treated as part of the institution's critical digital infrastructure, subject to the same standards of resilience and incident response as other core systems.

Data protection officers have a parallel and complementary responsibility to ensure that all uses of generative AI comply with applicable data protection and AI-specific regulation, including GDPR and the EU AI Act. This requires a proactive approach to governance rather than retrospective compliance. Data Protection Impact Assessments must be conducted for AI deployments that involve personal data or pose heightened risks to rights and freedoms. These assessments should address not only data handling practices, but also issues of purpose limitation, data minimisation, retention, and downstream use.

Privacy-by-design and privacy-by-default principles must be embedded into all institutionally supported AI systems. Data protection officers are responsible for ensuring that contractual arrangements, technical configurations, and user guidance reflect these principles in practice. They must also ensure that clear audit trails are maintained, enabling accountability in the event of complaints, regulatory scrutiny, or incidents involving misuse or harm. In an AI context, accountability requires the ability to reconstruct decision pathways and data flows, even where automated systems are involved.

Both IT services and data protection officers play a critical role in the procurement and vetting of external AI vendors. Institutional procurement processes must extend beyond assessments of functionality and cost to include rigorous scrutiny of training data provenance, documented model limitations, bias mitigation strategies, environmental impact, and data governance arrangements. Vendors should be required to provide sufficient transparency to allow institutions to meet their legal and ethical obligations. Where such transparency cannot be secured, adoption should be reconsidered, irrespective of perceived technical advantage. In cases where adoption proceeds despite identified limitations or risks, IT services must ensure that the rationale for these decisions is formally documented and communicated. This includes making explicit what compromises have been accepted, on what grounds, and with what mitigations in place, so that staff can have confidence that departures from ethical values have been carefully considered and justified, and that such decisions remain subject to review if more ethically robust alternatives become available.

Close collaboration between IT services, data protection officers, legal teams, and academic leadership is essential to effective AI governance. Generative AI systems do not sit neatly within existing organisational silos, and fragmented oversight increases institutional risk. Technical and compliance staff should be embedded in decision-making processes related to AI strategy, ensuring that governance considerations are integrated from the outset.

Through the fulfilment of these responsibilities, IT services and data protection officers ensure that generative AI adoption within higher education is aligned with institutional values. Their work makes it possible for teaching and learning communities to engage with AI confidently, knowing that appropriate safeguards and regulatory protections are in place.