# Cyber-Ethical Leadership in Higher Education

## A Practice-Based Framework for the Digital Age

**Ryma Abassi,**

University of Carthage, SUPCOM, INNOVCOM
Research Lab Tunis, Tunisia

Published Dec. 2025

**Keywords**

Higher education, cybersecurity, ethics, leadership, digital

## Abstract

The rapid digitization of higher education has introduced complex ethical challenges that demand new forms of leadership. This paper explores the concept of cyber-ethical leadership as a critical response to evolving issues such as data privacy, AI-generated academic content, digital surveillance, and cybersecurity crisis management. Drawing from real-world case studies and institutional practices, we propose a practice-based framework that emphasizes ethical reflexivity, participatory governance, and multi-stakeholder engagement. By reframing leadership as ethical agency rather than hierarchical authority, this study highlights how leaders in academia can navigate digital dilemmas through context-aware, inclusive decision-making. The findings call for the integration of digital ethics into institutional policy, leadership training, and crisis preparedness, contributing to a more resilient and ethically grounded digital transformation of higher education.

---

Corresponding author: Dr Ryma Abassi, Associate Professor and Director at ISETCOM University of Carthage, Email: ryma.abassi@supcom.tn.

How to quote this article: Abassi, Ryma. 2025. “Cyber-Ethical Leadership in Higher Education: A Practice-Based Framework for the Digital Age”, *Journal of Ethics in Higher Education* 7.2(2025): 79–101. DOI: https://doi.org/10.26034/fr.jehe.2025.8994 © the Author. CC BY-NC-SA 4.0. Visit: https://jehe.globethics.net

# 1 Introduction

As digital technologies increasingly integrate every aspect of higher education, the role of leadership is being redefined in real time. Institutions are no longer solely physical spaces for learning and governance, but they are now complex, interconnected digital ecosystems. From student data protection to the ethical deployment of artificial intelligence, university leaders are facing a growing number of decisions that challenge traditional rule-based leadership models. These decisions often occur in fast-moving, high-stakes environments where legal guidelines are evolving, ethical norms are debated, and technical expertise is essential.

The concept of cyber-ethical leadership has recently emerged as a critical corrective to the fast-moving ethical and governance gaps created by data-intensive business models, generative AI, pervasive surveillance, and escalating cyber crises. Contemporary studies argue that leaders must combine traditional ethical leadership practices with domain-specific competencies promoting data dignity and privacy by design and steering organizational decisions that limit extractive surveillance practices. Recent literature on AI and higher education highlights how generative models undermine conventional assessment and integrity frameworks, prompting calls for leadership that sets clear norms for acceptable AI use, re-designs assessment, and invests in staff training and institutional policies (Makanadar, 2024). At the intersection of governance and crisis response, (Bittle and El-Gayar, 2025) emphasize that ethical leaders enable resilient cybersecurity by embedding accountability, transparency, and multi-stakeholder coordination into incident preparedness and crisis management routines. (Panteli et al, 2025) reviews of ethical leadership in the AI era recommend practical frameworks that fuse ethical principles with technical oversight—urging leaders to translate abstract values into procurement rules, risk assessments, and operational practices that mitigate harms while preserving innovation.

Leadership in such contexts cannot rely on fixed codes or abstract ethical frameworks alone. Instead, it demands a form of practical wisdom, grounded in lived experience and adaptive judgment. In this article, we propose a practice-based approach to ethical leadership emphasizing action, context, and ethical reflexivity. This approach is essential for navigating the emerging dilemmas in digital higher education in contrast to rule-based systems that apply general principles regardless of context, a practice-based approach views ethical decision-making as dynamic, participatory, and deeply human.

This shift is particularly urgent in the domain of cybersecurity and digital governance, where institutional leaders must make decisions with far-reaching consequences. These include whether and how to use surveillance systems on campus, how to respond to data breaches, how to manage AI-generated academic content, and how to design policies that align technological capabilities with core institutional values.

Recent research underscores the urgent need for robust policy and governance frameworks to guide ethical leadership in the digital age, particularly in response to challenges such as AI ethics, data privacy, and cybersecurity. Existing global initiatives—like the EU's General Data Protection Regulation (GDPR), the OECD AI Principles (2019), and UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021) that establish normative foundations for transparency, accountability, and human-centered digital governance. These frameworks emphasize leaders' responsibilities to ensure fairness, prevent algorithmic bias, and protect individual rights within data-driven environments. However, their implementation often remains uneven, revealing a gap between high-level ethical commitments and practical enforcement mechanisms. Studies highlight that while GDPR has improved data governance maturity, organizations still struggle to embed ethical reflexivity into decision-making and leadership structures.

In parallel, emerging cybersecurity and AI governance models stress the role of ethical leadership in crisis management, resilience building, and responsible innovation. The NIST Cybersecurity Framework (2023 update), for instance, integrates ethical dimensions of risk governance, advocating for cross-sector collaboration and transparency in digital incident response. Similarly, national AI strategies in countries such as Canada, Singapore, and the UK increasingly incorporate ethics-by-design approaches to align innovation with societal values. Yet, researchers (e.g., Floridi, 2023; Stahl,

2024) argue that these frameworks remain fragmented and reactive, lacking the integrative vision needed for “cyber-ethical leadership.” This emerging paradigm calls for leaders who not only comply with regulatory standards but also cultivate cultures of trust, inclusivity, and moral responsibility in digital governance, bridging the persistent divide between technological advancement and ethical accountability

This paper presents a model of cyber-ethical leadership grounded in practice. It builds on both theoretical frameworks and real-world case studies to propose a pragmatic, human-centered method for decision-making in complex digital environments. By drawing from philosophy, cybersecurity governance, and educational leadership, this approach bridges the gap between normative ideals and institutional action. It aims to support current and future leaders in building resilient, ethically sound organizations in an era of rapid technological change.

The remaining part of this paper is organized as follows. Section 2 presents the theoretical foundations of the study. Section 3 examines the cyber-ethical landscape in higher education. Selected case studies are outlined in Section 4. Section 5 introduces a practical framework for ethical decision-making. Section 6 offers a critical discussion, followed by conclusions and recommendations in Section 7.

# 2 Theoretical Foundations

## 2.1 Ethical Leadership: From Normative Theory to Situated Practice

The concept of ethical leadership has traditionally drawn upon a rich philosophical legacy. Classical models of ethics including deontology (Kant, 1785), utilitarianism (Mill, 1863), and virtue ethics (Aristotle, 4th century BCE) have all influenced how we understand the moral obligations of those in positions of power. These frameworks emphasize acting according to duty, maximizing collective well-being, or cultivating moral character, respectively.

In institutional contexts such as higher education, these ethical frameworks are often translated into codes of conduct, regulatory standards, and strategic policy documents designed to ensure responsible behavior and accountability. Ethical leadership, in this traditional lens, is often associated with qualities such as honesty, fairness, transparency, and integrity (Brown & Treviño, 2006; Northouse, 2018).

However, the dynamic realities of the digital age expose the limitations of rule-based approaches when applied to contexts like cybersecurity, artificial intelligence, and digital surveillance. These fields evolve rapidly, often outpacing existing regulations or ethical codes. Leaders frequently face ambiguous or novel situations for which no clear precedent or universal principle exists. As Bauman (1993) argues, modern ethical life is characterized by uncertainty, and this moral ambivalence requires more than adherence to formal rules, it demands ongoing ethical deliberation.

(Starratt, 2004; Ciulla, 2020) acknowledge that ethical decision-making is often non-linear, relational, and deeply contextual. In this view, leadership ethics are not simply applied from above but are co- constructed with stakeholders, shaped by real-time conditions and institutional culture. Heifetz (1994) distinguishes between technical problems, which can be solved with expertise, and adaptive challenges, which require learning, experimentation, and values-based judgment. Cyber-ethical dilemmas, such as whether to disclose a data breach or how to regulate AI in assessments, often fall in the latter category.

Consequently, ethical leadership in higher education must expand its focus from static ideals to include ethical agility and the capacity to make responsible decisions under uncertain conditions while remaining aligned with core values. This requires a shift from what is prescribed to what is practiced, and from a model of leadership based on control to one based on ethical responsiveness.

## 2.2 The Practice-Based Turn in Governance and Leadership

The practice-based approach to leadership represents a paradigmatic shift in how ethical behavior is understood within organizations. Rather than viewing leadership as a set of personal traits or compliance with predefined rules, practice theorists argue that leadership emerges through socially embedded, iterative, and context-sensitive actions (Feldman & Orlikowski, 2011; Gherardi, 2009).

This perspective builds on the foundational principles of practice theory (Schatzki, 2001; Reckwitz, 2002). It views practices as configurations of materially and socially organized activities through which meaning, knowledge, and normative frameworks are enacted, negotiated, and reproduced. As (Nicolini, 2013) explains, leadership is not something people "have" but something they "do" through relational interaction, material engagement, and situated improvisation.

When applied to ethical leadership, this approach implies that norms and values are not merely applied but they are performed, negotiated, and institutionalized through action. In other words, ethics becomes an ongoing process rather than a static framework. For instance, responding to a cyberattack is not only a technical exercise but a moral one: how transparently should we communicate with stakeholders? What trade-offs are acceptable between risk mitigation and privacy? These are not questions that can be resolved through policy alone—they require the exercise of ethical judgment in context.

This transition corresponds to the emergence of a "rule-of-practice" order, as outlined in the call for papers, wherein norms and rules are not predefined but instead emerge through and because of practice itself. In such a model, ethical leadership entails fostering a culture of inquiry, reflection, and adaptive learning, rather than enforcing top-down compliance. This is particularly relevant in cyber-ethical domains, where leaders must respond to evolving threats, negotiate with multidisciplinary teams, and make decisions that often carry no clear right or wrong answers.

Moreover, practice-based leadership supports the development of distributed ethical capacity. Instead of centralizing ethical decision-making in executive offices, institutions can cultivate ethical agency across all levels, encouraging faculty, students, IT staff, and administrative leaders to engage in ethical reflection and dialogue. This democratization of ethical leadership is particularly vital in educational contexts, where modeling participatory, values-driven leadership reinforces the very mission of the university.

# 3 The Cyber-Ethical Landscape in Higher Education

The digital transformation of higher education has brought unprecedented opportunities for innovation, collaboration, and access. However, it has also introduced a complex landscape of cyber-ethical challenges that academic institutions must address with deliberate and principled leadership.

## 3.1 Key Areas of Ethical Risk

Four key areas can be considered: Data Privacy and Personal Data Management, academic integrity, monitoring vs. autonomy and cybersecurity incident handling.

*Data Privacy and Personal Data Management*

Universities sensitive records, from transcripts to health disclosures and financial aid applications. In 2018, the University of Greenwich in the U.K. suffered a ransomware attack that exposed student data; the Information Commissioner's Office fined them £120,000 for failing to protect personal information under GDPR standards (Lallie et al, 2023).

*Academic Integrity and AI-Generated Content*

Generative AI tools like ChatGPT and others have blurred the line between original work and machine-assisted output. In 2023, several thousand students at a major U.S. university were flagged by Turnitin's AI-detector for submitting essays that closely matched GPT-generated text (Pratschke, 2024). The institution revised its syllabus to require students to annotate any AI "contributions" and redesigned assessments around in-class presentations and portfolios.

*Monitoring vs. Autonomy: Surveillance Technologies and Trust*

In an effort to mitigate academic dishonesty and enhance security, educational institutions are increasingly adopting invasive surveillance technologies, often raising significant concerns regarding the protection of individual privacy. During the COVID-19 pandemic, online proctoring software were used by institutions such as Western University in Canada and Rutgers University in the U.S (Balash et al, 2021). These universities adopted tools like Proctorio and Respondus Monitor, which use AI to monitor students via their webcams, track eye movements, record screens, and even analyses keystroke patterns. This sparked widespread concern among students and faculty about privacy violations, potential bias in AI algorithms, and data security risks, leading to petitions and legal complaints. In several cases, universities were forced to review or even suspend the use of such technologies due to pressure from student unions and digital rights organizations like the Electronic Frontier Foundation (EFF).

*Cybersecurity Incident Handling: Who Decides, How, and with What Trade-offs?*

When attacks strike, institutions face wrenching choices under pressure. In 2020, the University of Utah paid over $457,000 in Bitcoin to recover encrypted files after a Ryuk ransomware breach (Westbrook, 2021). Post-incident reviews criticized the decision for lacking clear approval from the university's IT governance board. Now, protocols require multi-stakeholder authorization before any ransom payment. After Maastricht University's 2019 breach, leadership initially withheld details from staff; once the scale became apparent, the abrupt public disclosure eroded trust. The university has since adopted a "transparent by default" policy: informing affected community members within 48 hours of any confirmed breach (Lückerath- Rovers, 2024).

## 3.2 Emerging Leadership Dilemmas

By grounding each risk and dilemma in concrete cases, higher-education leaders can better anticipate challenges, adopt proven safeguards and maintain trust as they steer their institutions through the evolving cyber-ethical landscape.

Balancing Innovation with Responsibility: While advanced technological tools have the potential to provide substantial benefits, their deployment may also introduce unintended and potentially detrimental consequences. Georgia State University’s predictive-analytics program flagged students as “at-risk” based on historical data that inadvertently penalized first-generation and minority students (Kurn et al, 2023). In response, GSU paused the initiative, engaged sociologists and ethicists to audit its algorithms, and introduced bias-mitigation steps before relaunch.

Pressure from External Stakeholders vs. Institutional Values: Partnerships and funding can clash with academic freedom or privacy. In 2021, UCLA’s collaboration with a data-analytics firm led to a push for campus-wide user profiling; student governments and faculty senates pushed back, citing mission conflicts, and UCLA ultimately scaled back the deployment to a single pilot course with full opt-in consent (UCLA 2021).

*Leadership in Uncertainty: Ethical Response Under Cyber Crisis Conditions*
Rapidly evolving threats force leaders to make high stakes calls with incomplete data. During Notre Dame’s March 2024 ransomware event, leadership delayed notifying the campus for 72 hours to verify scope—drawing criticism for leaving staff and students uninformed. The university has since committed to a 24-hour “initial notice” protocol, clarifying what is known and what remains under investigation (Notre dame, 2024).

# 4 Case Studies

This section presents real-world case studies that illustrate the ethical complexities faced by higher education institutions in the digital age. Each case highlights a specific challenge ranging from data breaches to AI integration and digital surveillance and explores how leadership responses shaped outcomes and ethical learning.

## 4.1 Case 1: Data Breach in a University System

*Context and Incident Overview*
In September 2020, the University of Utah fell victim to a Ryuk ransomware attack that encrypted critical systems including payroll, student records, and research databases and demanded a payment of 0.14 BTC (approximately

$457,000 at the time) to restore access. The breach exploited an unpatched virtual private network (VPN) appliance and spread laterally across the campus network within 48 hours (Westbrook, 2021).

### *Ethical and Operational Response*

The university's incident response team immediately activated its cyber-incident playbook, convening a cross- functional Cybersecurity Governing Board composed of IT, legal, ethics, and academic affairs representatives. Ethically, the decision to pay ransom was weighed against the duty to protect stakeholder data, the risk of funding criminal activity, and the imperative to restore educational services. Operationally, containment measures included isolating affected subnets, taking backups offline, and engaging a third-party forensic firm. Post-incident, the institution instituted an ethical review of its decision-making process, acknowledging that the "least-harm" principle justified the payment only after all technical recovery options had been exhausted.

### *Communication Strategy and Stakeholder Management*

Leveraging principles from risk-communication theory, the university issued a tiered disclosure:

1. Initial Notice (Day 1): A brief alert to faculty, staff, and students indicating that systems were offline due to a "cybersecurity event," without speculative details.
2. Situation Update (Day 3): Confirmation of ransomware involvement, estimated restoration timelines, and guidance for interim manual processes.
3. After-Action Report (Day 30): A comprehensive retrospective detailing root-cause analysis, lessons learned, and new controls (multi-factor authentication, quarterly tabletop exercises).

Key stakeholders, including student government, research directors, and the local press, were invited to a virtual town hall. This transparent approach mitigated rumours, preserved institutional trust, and exemplified an ethical commitment to both accountability and learning.

### 4.2 Case 2: Integrating Generative AI into Student Evaluation

Context and Governance Gaps: In early 2024, the University of Hong Kong piloted an AI-augmented writing-assessment tool that provided automated feedback on student essays (Wong and Chan, 2025). The absence of an overarching AI-use policy led to uncertainty: instructors were unsure whether to grade based on AI-generated suggestions or solely on student-authored text; students were unclear about disclosing AI contributions; and the data-governance structure lacked provisions for retaining AI-model prompts.

Ethical Questions: Three principal ethical concerns emerged:

1. Fairness & Bias: The AI model was trained on predominantly Western academic corpora, risking culturally insensitive feedback for non-native English writers.
2. Transparency & Accountability: Without clear audit trails, it was impossible to determine whether a grade reflected the student's critical thinking or the AI's wording.
3. Consent & Autonomy: Students expressed discomfort that their original voice might be supplanted by machine-generated prose, potentially undermining epistemic integrity.

#### *Building Participatory Policy Through Practice*

To address these gaps, the university convened a "Generative AI in Assessment" working group comprising students, faculty, instructional designers, data-ethicists, and IT security officers. Over three iterative workshops, the group:

1. Mapped Stakeholder Needs: Elicited perspectives on learning objectives, equity, and privacy.
2. Co-Drafted Usage Guidelines: Defined clear boundaries and required students to append a "AI Usage Statement" to every submission. For example, AI may suggest stylistic edits but not restructure arguments.
3. Piloted & Refined: Deployed the policy in two writing-intensive courses, collected anonymous feedback, and adjusted the guidelines

to clarify disclosure procedures and establish an appeals process for disputed grades.

This participatory model not only closed initial governance gaps but also fostered a shared sense of ownership and ethical reflection among the academic community.

### 4.3 Case 3: Surveillance Cameras in Classrooms

Security Needs vs. Academic Freedom: A mid-sized European technical university installed high-definition cameras in 50 high-risk laboratories to deter equipment theft and ensure rapid response to safety incidents (chemical spills, equipment malfunctions) (Kissoon and Karran 2024). While the cameras operated only during after-hours, their placement in research spaces sparked concerns that researchers and students would self-censor discussions or experiments for fear of constant monitoring.

Staff and Student Pushback: Listening as an Ethical Act: After an anonymous survey revealed that 72 % of graduate students felt “uncomfortable” and 45 % believed their intellectual freedom was compromised, the university initiated a series of “listening sessions” with affected departments. These forums were structured around principles of dialogic ethics:

1. Active Listening: Administrators and security staff served solely as note-takers, allowing researchers to express concerns without interruption.
2. Joint Problem-Definition: Participants collaborated to identify specific scenarios where cameras produced more harm than benefit e.g. during confidential thesis defences.
3. Co-Constructed Mitigations: Agreed solutions included motion- activated recording rather than continuous capture, automatic anonymization of video streams for non-urgent review, and a clear “no-camera” policy for academic presentations and peer-review meetings.

The outcome was a revised surveillance policy that balanced the campus’s duty of care with respect for intellectual autonomy. Importantly, by treating listening as an ethical intervention, leadership reinforced trust and demonstrated that surveillance could be both responsible and rights-respecting.

# 5 Building a Practice-Based Framework

## 5.1 Components of the Model

Ethical Reflexivity and Situational Awareness: Ethical reflexivity refers to the capacity of individuals and institutions to continuously examine their own actions, assumptions, and decisions in response to changing technological contexts. This requires a dynamic, situational awareness where ethical considerations are not static, but evolve as new technologies, threats, and societal needs emerge. Leaders must not only react to issues as they arise but also anticipate ethical challenges through continuous reflection. This could include creating spaces for regular reflection, engaging in self-assessment practices, and cultivating a culture of inquiry where ethical questions are integral to decision-making processes.

For example, universities like Stanford University have embedded ethical reflexivity into their decision-making by having senior leaders meet periodically to discuss technological advancements and their potential ethical implications, often in consultation with ethicists, philosophers, and technology experts.

*Multi-Actor Engagement (Students, Faculty, IT, Governance)*

A truly ethical approach in higher education necessitates the inclusion of diverse perspectives from multiple stakeholders in decision-making. This includes students, faculty, IT professionals, and governance bodies, all of whom have distinct yet complementary insights into the ethical challenges posed by technology. For instance, students may raise concerns regarding privacy, while faculty may be focused on academic integrity, and IT teams on technical vulnerabilities. Effective decision-making must foster collaboration and communication among these groups to ensure that all viewpoints are accounted for and ethical outcomes are achieved.

For example, the University of California system uses a “digital governance framework” that involves students, faculty, and IT staff in regular consultations about cybersecurity measures, including annual forums where key stakeholders discuss upcoming tech initiatives.

### *Institutional Memory and Documentation of Ethical Decisions*

For an institution to build long-term ethical resilience, it must maintain a strong institutional memory. This means systematically documenting ethical decisions made across various technology-related projects, whether related to cybersecurity incidents, AI policy implementation, or digital surveillance. These records serve not only as a historical archive but also as a learning tool for future decision-making. Documenting the rationale behind decisions, the engagement process, the outcomes, and the ethical dilemmas faced helps institutions avoid repeating past mistakes and fosters accountability.

For example, Harvard University’s Data Privacy Office maintains detailed records of every significant decision made regarding student data handling, including the ethical considerations discussed and the outcomes. These records are made accessible to future leadership to inform ongoing policy development.

### *Tools: Crisis Simulation, Ethical Impact Assessments, Participatory Governance*

Practical tools are critical in embedding ethics into everyday decision-making in higher education. Crisis simulations, where institutions practice responses to cyber-attacks or data breaches, help prepare leadership for real-world ethical dilemmas. Ethical impact assessments, similar to environmental impact assessments, can be applied to new technologies, policies, or systems to evaluate potential harms before implementation. Participatory governance mechanisms, such as advisory boards with students, staff, and external stakeholders, can also be used to ensure that decisions are ethical and transparent.

For example, the University of Edinburgh conducts annual crisis simulations where faculty, IT, and governance teams collaborate to respond to hypothetical data breaches, helping to ensure that ethical and operational responses are well-coordinated. Moreover, several universities, including the University of Toronto, have developed ethical impact assessments for their AI initiatives, using these to evaluate the risks of bias, fairness, and accountability before deploying new systems.

## 5.2 Practical Recommendations

Create Standing Digital Ethics Committees: To ensure that ethical concerns are consistently integrated into the digital transformation process, universities should establish permanent digital ethics committees. These committees would be tasked with evaluating the ethical implications of new technologies, overseeing data privacy policies, and providing ongoing guidance on emerging digital risks. Composed of a diverse group, including ethicists, technologists, students, and administrators, these committees would ensure that ethics are embedded in the strategic planning of digital initiatives.

For example, the University of Oxford has a Digital Ethics Advisory Board that regularly reviews the ethical implications of new technologies implemented on campus. The board offers recommendations on everything from AI to data governance, with a particular focus on student privacy and academic integrity.

### *Incorporate Cybersecurity and Digital Ethics into Leadership Training*

For digital ethics to be successfully integrated into university operations, leadership at all levels must be equipped with both cybersecurity awareness and a robust understanding of the ethical challenges of digital technologies. This can be achieved through leadership training that incorporates case studies, best practices, and frameworks for responding to ethical dilemmas in a digital context. This training should also focus on the ethical principles of transparency, accountability, and equity. For instance, the University of California, Berkeley, has incorporated digital ethics modules into its leadership development programs. Senior administrators are trained to understand the implications of cybersecurity decisions on privacy and academic freedom, ensuring that they can make well-informed, ethical choices in the face of technological disruptions.

*Develop Flexible, Context-Aware Institutional Policies*

As digital technologies evolve, so too must institutional policies. Universities should avoid creating rigid, one-size-fits-all rules. Instead, they should develop flexible policies that can be adapted to different contexts, whether responding to a cybersecurity threat, integrating AI in classrooms, or balancing surveillance and privacy concerns. These policies should be designed to evolve with new technologies and societal shifts, ensuring they remain relevant and effective.

The Massachusetts Institute of Technology (MIT) has a flexible policy framework for AI use, which allows for rapid adaptation based on emerging technologies and student concerns. MIT's AI policy is reviewed annually by a multi-disciplinary team to ensure that it reflects the latest academic, technological, and ethical developments.

Align Digital Transformation with Human-Centered Values: As institutions undergo digital transformation, it is essential that technology serves to enhance, rather than undermine, the human experience in higher education. This means aligning digital strategies with human-centered values such as equity, accessibility, and academic freedom. Decisions around digital tools and policies must prioritize the well-being of students, faculty, and staff and foster an environment of trust, inclusion, and respect for autonomy.

The University of Michigan's digital transformation strategy emphasizes human-centered design, ensuring that all technological upgrades are accessible to diverse student populations, including those with disabilities, and that new platforms uphold principles of academic integrity and fairness. The university has embedded principles of accessibility and inclusivity into all major digital initiatives, ensuring that technological change advances the common good.

## 6 Discussion

In the context of digital transformation in higher education, traditional leadership models—characterized by hierarchical authority, centralized decision-making, and control—are increasingly inadequate. The rising complexity of ethical challenges in the digital domain, including issues related to data privacy, artificial intelligence, and cybersecurity, necessitates a paradigm shift in leadership approaches. Ethical leadership in the digital era should transition from directive, top-down models toward frameworks grounded in ethical agency. Such models emphasize active engagement, critical reflection, and collaborative decision-making processes to effectively navigate the evolving digital landscape. Ethical agency refers to the capacity of leaders to recognize their moral responsibilities and to act in ways that promote the welfare of all stakeholders, including students, faculty, staff, and society at large. This shift requires leaders to not only navigate complex ethical challenges but to also cultivate ethical awareness in their teams, encouraging open dialogue and participatory decision-making. In this reframed approach, leadership is less about providing clear-cut answers and more about fostering environments where ethical issues can be openly discussed, analyzed, and addressed collectively.

For instance, the ethical leadership model at institutions like MIT and the University of California encourages leaders to take responsibility not just for decisions but also for the broader ethical implications of technological advancements. These institutions have begun to focus more on cultivating ethical leadership skills among senior administrators, ensuring that leaders approach challenges not with a purely managerial mindset but with an ethical lens that takes into account the broader societal, cultural, and academic implications of digital technologies.

Besides, an important aspect of ethical leadership in higher education is the notion of "practice as pedagogy." This concept suggests that leaders learn and develop their ethical competencies not through theoretical instruction alone but through active, reflective engagement in real-world scenarios. Just as students in higher education learn through practice and experience, so too must leaders in educational institutions refine their ethical skills through engagement with the complexities of daily decision-making.

For example, when a university faces a data breach or a cybersecurity incident, it is not enough for leaders to rely on abstract ethical frameworks. Instead, they must navigate the situation in real-time, balancing the competing demands of transparency, accountability, privacy, and operational efficiency. This practical engagement with ethical dilemmas allows leaders to learn by doing, refining their judgment, fostering ethical sensitivity, and improving their ability to handle similar challenges in the future.

Moreover, leadership training programs that incorporate case studies, ethical simulations, and crisis management scenarios can help prepare leaders for the ethical challenges they are likely to face. These types of experiential learning opportunities allow leaders to practice ethical decision-making in a controlled, reflective environment, thereby enhancing their ability to make sound ethical choices in the real world.

Research shows that institutions that provide leaders with opportunities to practice ethical decision-making, such as through crisis management simulations or ongoing training in digital ethics, foster more adaptive and effective ethical leadership. For instance, universities like the University of Toronto have incorporated ethics simulations in their leadership programs, where administrators must deal with hypothetical ethical scenarios, giving them a chance to practice and refine their decision-making processes.

Moreover, while the practice-based approach to ethical leadership provides substantial benefits, it is not without its risks and limitations. One key limitation is the potential for leaders to rely too heavily on ad-hoc decision-making without grounding their actions in established ethical principles. In high-pressure situations, such as cybersecurity crises or the rapid adoption of AI technologies, leaders might make decisions based on immediate operational needs rather than long-term ethical considerations. This could lead to decisions that prioritize convenience, efficiency, or short-term gains over fundamental ethical principles, such as fairness, transparency, and privacy.

Another risk is the potential for inconsistency in ethical decision-making. Without clear, formalized ethical guidelines and frameworks, leaders might interpret ethical dilemmas differently, leading to a lack of cohesion in institutional responses to issues. This could result in conflicting decisions, creating confusion and undermining trust among stakeholders, including students, faculty, and external partners.

For instance, during the deployment of surveillance technologies in classrooms, different leaders might have varying perspectives on what constitutes an acceptable level of surveillance, leading to inconsistent policies or practices. Some might prioritize security, while others might emphasize privacy or academic freedom. This inconsistency can lead to dissatisfaction and disengagement from both students and faculty, who may feel that their voices are not adequately represented in decision-making processes.

Moreover, a purely practice-based approach may also overlook the importance of theoretical grounding in ethics. Ethical theories, frameworks, and principles provide essential guidance for leaders, helping them to navigate complex moral dilemmas in a structured way. While practice offers valuable learning experiences, it should be complemented by a solid understanding of ethical principles, ensuring that decisions are made with a comprehensive awareness of their moral implications.

To mitigate these risks, institutions must strike a balance between practice and theory. While experiential learning through ethical simulations and real-world crises is crucial, leaders must also be well-versed in ethical frameworks and the core values of the institution. Ethical training should therefore combine practical engagement with a deep understanding of ethical principles, ensuring that leaders have the tools and insights needed to make well-reasoned, consistent, and ethically sound decisions.

The discussion highlights the need for a paradigm shift in leadership within higher education, from a model rooted in authority and control to one based on ethical agency, collaboration, and reflective practice. Leaders must be able to navigate the complexities of digital ethics not through theoretical knowledge alone but through active engagement with real-world challenges. However, the potential risks of a purely practice-based approach underscore the importance of grounding decision-making in established ethical principles and frameworks. A balanced approach integrating both practice and theory will enable leaders to address ethical challenges with greater insight, consistency, and accountability, ultimately advancing the mission of higher education in the digital age.

# 7 Conclusion

As digital technologies become ever more central to the mission of higher education, institutions must cultivate cyber-ethical leadership that is both proactive and inclusive. Core challenges ranging from data privacy and academic integrity to AI-driven evaluation and pervasive surveillance, demand robust ethical frameworks that are fully consonant with foundational academic principles, including equity, transparency, and freedom of inquiry.

Central to this endeavour is the institution of inclusive governance structures that bring together students, faculty, IT specialists, and senior administrators in collaborative ethical deliberation. By embedding formal mechanisms for continuous ethical reflection such as multidisciplinary ethics committees, regular stakeholder forums, and systematic documentation of decisions, universities can strengthen accountability and foster mutual trust across their communities.

Moreover, resilience in the face of rapid technological evolution requires that universities adopt flexible, adaptive policy architectures. These architectures should be informed by empirical case studies and best practices, and supported by ongoing digital ethics training for leadership at all levels. Through a participatory, principle-driven approach to policy design and implementation, higher education institutions will be better equipped to safeguard their ethical foundations and to lead responsibly amidst the complexities of the digital age.

# 8. Bibliography

Aristotle. 2009. *Nicomachean Ethics* (translated by W.D. Ross). Oxford University Press.

Balash, D. G., Kim, D., Shaibekova, D., Fainchtein, R. A., Sherr, M., & Aviv, A. J. 2021. Examining the examiners: Students' privacy and security perceptions of online proctoring services. In *Seventeenth symposium on usable privacy and security* (SOUPS 2021), 633–652.

Bauman, Z. 1993. *Postmodern Ethics*. Blackwell.

Brown, M. E., & Treviño, L. K. 2006. Ethical leadership: A review and future directions. *The Leadership Quarterly*, 17(6), 595–616.

Bittle, K., & El-Gayar, O. 2025. Generative AI and Academic Integrity in Higher Education: A Systematic Review and Research Agenda. *Information*, *16*(4), 296. https://doi.org/10.3390/info16040296

Ciulla, J. B. 2020. *Ethics, the Heart of Leadership* (3rd ed.). Praeger.

Feldman, M. S., & Orlikowski, W. J. 2011. Theorizing practice and practicing theory. *Organization Science*, 22(5), 1240–1253.

Floridi, L. 2023, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford: Oxford Academic, Online Ed., 24 Aug. 2023.

Gherardi, S. 2009. Introduction: The critical power of the 'practice lens'. *Management Learning*, 40(2), 115–128.

Heifetz, R. A. 1994. Leadership Without Easy Answers. Harvard University Press.

Kissoon, C., & Karran, T. 2024. Universities' over-monitoring culture is a threat to academic freedom. *Times Higher Education*. https://www.timeshighereducation.com/blog/universities-over-monitoring-culture-threat-academic-freedom

Kurni, M., Mohammed, M. S., & Srinivasa, K. G. 2023. Predictive analytics in education. In *A Beginner's Guide to Introduce Artificial Intelligence in Teaching and Learning*, Cham: Springer International Publishing, 55–81.

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. 2023. Understanding Cyber Threats Against the Universities, Colleges, and Schools. arXiv preprint arXiv:2307.07755.

Lo, N., Wong, A., & Chan, S. 2025. The Impact of Generative AI on Essay Revisions and Student Engagement. *Computers and Education Open*, 100249.

Lückerath-Rovers, M. 2024. The Case of Maastricht University Paying Ransom After a Cyber Attack. In *Moral Dilemmas in the Boardroom: Striking the Balance in Ethical Decision Making.* Cham: Springer Nature Switzerland, 155–164.

Makanadar, A. Digital surveillance capitalism and cities: data, democracy and activism. *Humanit Soc Sci Commun* 11, 1533 (2024).

Nicolini, D. 2013. *Practice Theory, Work, and Organization: An Introduction*. Oxford: Oxford University Press.

Northouse, P. G. 2018. *Leadership: Theory and Practice* (8th ed.). Sage.

Notre Dame. 2024. https://cyberpress.org/fog-ransomware-notre/?utm_source=chatgpt.com#google_vignette

Panteli, N., Nthubu, B.R. & Mersinas, K. 2025. Being Responsible in Cybersecurity: A Multi-Layered Perspective. *Inf Syst Front*. https://doi.org/10.1007/s10796-025-10588-

Pratschke, B. M. 2024. *Assessing Learning. In Generative AI and Education: Digital Pedagogies, Teaching Innovation and Learning*. Cham: Springer Nature Switzerland. Design, pp. 91–108.

Reckwitz, A. 2002. Toward a theory of social practices: A development in culturalist theorizing. *European Journal of Social Theory*, 5(2), 243–263.

Schatzki, T. R. 2001. *The Practice Turn in Contemporary Theory*. Routledge.

Stahl, B. C., & Eke, D. 2024. The ethics of ChatGPT–Exploring the ethical issues of an emerging technology. *International Journal of Information Management*, *74*, 102700.

Starratt, R. J. 2004. *Ethical Leadership*. Jossey-Bass.

UCLA. 2021. Faculty call for pause on budget & network security changes at UCLA, Website. https://uclafa.org/2021/06/09/faculty-knock-centralization-plans/?utm_source=chatgpt.com

Westbrook, A. D. 2021. A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets and Defending National Security. NYUJL & Bus., 18, 391.

## 9. Short biography

Dr. Ryma Abassi is Associate Professor and Director at ISETCOM, the first woman in this role, and researcher at SUP'COM. A Fulbright Scholar at Tufts University (2017) and SSHN awardee (2014, 2017), she is a leading cybersecurity expert in Africa and the Middle East. She authored three books, published over 70 papers, and is co-supervising six PhD students. Recognized in the 2024 SIA WISF Power 100, she focuses on cybersecurity, AI, trust management, IoT, and security protocol validation.

Email: ryma.abassi@supcom.tn