rmp

Risk Control

Strengthening Resilience Against Financial Crime

In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

Strengthening Resilience Against Financial Crime

Introduction

UK Higher Education Institutions (HEIs) operate within a complex and increasingly vulnerable financial landscape. With significant public funding, international partnerships, devolved governance, and high-volume transactions across student finance, procurement, and donations, HEIs face multifaceted risks that extend well beyond traditional notions of fraud.

Recent high-profile incidents have brought these risks to the forefront. In one such case, the University of West London became the focal point of £6.2 million in fraudulent student loan applications — the majority tied to its franchised partner, Oxford Business College. Elsewhere, students have been convicted for laundering drug money through institutional payment systems, exploiting weaknesses in oversight and detection. These examples signal an urgent need for HEIs to reframe financial crime not as an isolated threat, but as a persistent and evolving governance challenge.

This document provides comprehensive guidance on how HEIs can embed fraud resilience into core operations, strategic oversight, and institutional culture. It examines legal obligations under the UK's Failure to Prevent Fraud offence, sector-specific vulnerabilities, and practical methods to foster proactive risk management. Importantly, it encourages institutions to look beyond compliance — advocating for a values-driven, prevention-first approach that aligns with the ethical standards expected of publicly funded education providers.

As the sector continues to engage with global markets, adapt to digitalisation, and navigate funding pressures, building a robust defence against financial crime must be recognised as both a compliance necessity and a moral imperative.

This evolving risk environment is now shaped by new legal obligations introduced through **Section 199 of the Economic Crime and Corporate Transparency Act 2023 (ECCTA)**. Coming into force on 1 September 2025, the **Failure to Prevent Fraud** offence establishes criminal liability for large organisations where an associated person, such as a staff member, student, contractor, or academic partner, commits a fraud offence intended to benefit the institution or its clients.

Notably, this is a **strict liability offence**. There is no requirement to prove knowledge or intent by senior leadership; liability arises solely from the failure to prevent. HEIs fall into scope if they meet two out of three criteria:

— 250 or more employees.

— Over £36 million in annual turnover.

— More than £18 million in total assets.

Defence is only available where institutions can demonstrate that **reasonable prevention procedures** were in place, or that such procedures were not reasonably expected given the circumstances. While smaller HEIs may fall outside the formal scope, the principles of the offence, and the reputational risks it represents, apply sector-wide[1].

Legal Obligations and Fraud Prevention Framework

The introduction of the **Failure to Prevent Fraud** offence under Section 199 of the **Economic Crime and Corporate Transparency Act 2023 (ECCTA)** redefines how organisational accountability for fraud is evaluated. From September 2025, HEIs that meet the statutory threshold may be held criminally liable if a person associated with them, including staff, students, contractors, or third-party providers, commits a fraud offence with intent to benefit the institution or its clients.

This applies even where senior leadership is unaware of the misconduct. The offence is based on **strict liability**, meaning institutions may be prosecuted solely for failing to prevent fraud unless adequate safeguards are in place. The law requires organisations to demonstrate that **reasonable and proportionate procedures** were in place or that such procedures could not reasonably be expected given the circumstances[2].

Crucially, the legislation does not require the institution to have known about the fraud for liability to arise. Instead, it places emphasis on whether the institution had taken adequate steps to prevent it. The government outlines six principles to guide the design and implementation of those procedures. These are explored below in a format aligned with Higher Education operations, with an emphasis on learning, accountability, and contextual relevance.

1 Proportionate Procedures

Institutions must ensure that fraud prevention procedures are appropriate to the risks faced and proportionate to their scale, complexity, and operational reach.

Effective proportionate procedures help HEIs:

— **Ensure controls reflect risk exposures**: Higher-risk activities, such as international student admissions, donation acceptance, or outsourced academic delivery, should receive deeper scrutiny than routine low-risk processes.

— **Avoid excessive burden while maintaining integrity**: Over-regulation of simple activities may create inefficiencies or erode engagement. Risk-sensitive calibration helps maintain protection without stifling core functions.

- **Promote clarity and usability**: Staff should understand which procedures apply and be able to implement them confidently. Documents, workflows, and systems must reflect real-world operations.

Institutions should document how procedures were selected based on the nature of identified risks, ensuring transparency and traceability in mitigation strategies[3].

2 Top-Level Commitment

Senior leadership must visibly and consistently champion fraud prevention. Without endorsement from the top, controls risk being sidelined or under-prioritised.

Strong top-level commitment enables HEIs to:

- **Reinforce ethical culture and behavioural expectations:** Leaders who speak openly about integrity and fraud resilience shape institutional norms and values.
- **Embed fraud prevention into strategic priorities:** Inclusion in university strategies, governance frameworks, and performance discussions signals that this is a non-negotiable part of institutional identity.
- **Allocate authority and resources appropriately:** Senior sponsorship helps direct funding and staffing to areas of emerging risk or procedural improvement, avoiding fragmentation or neglect.

Leadership engagement should be demonstrable in governance documentation, including strategy papers, risk assurance reports, and fraud response protocols, to satisfy ECCTA requirements[4].

3 Risk Assessment

Understanding fraud risk is central to designing meaningful and responsive controls. Institutions must identify where they are vulnerable, how risks may manifest, and what consequences may arise.

A robust risk assessment process enables HEIs to:

- **Map risk across operational domains:** From financial aid and donor engagement to recruitment partnerships and cyber operations; institutions must understand where exposure lies and how it evolves.
- **Include behavioural and cultural risk indicators:** Beyond structural weaknesses, institutions should consider how pressure, opportunity, or rationalisation may drive individuals toward misconduct.
- **Use assessment findings to drive action:** Documented risks should feed into procedures, escalation plans, and governance reports, not remain static or theoretical.

Risk assessments must be periodically reviewed and recalibrated in response to emerging typologies, incidents, and sector-wide intelligence — forming part of an auditable compliance cycle[5].

4 Due Diligence

Due diligence refers to the steps an institution takes to understand and verify the integrity, credentials, and conduct of individuals and organisations acting on its behalf. In the context of HEIs, this includes staff, contractors, academic partners, recruitment agents, donors, and any other associated persons.

Effective due diligence helps institutions:

- **Understand who they are working with: T**his includes verifying identities, assessing reputational history, and confirming legal standing.
- **Establish clear expectations and responsibilities:** Contracts and agreements should include clauses that outline fraud prevention obligations, cooperation with investigations, and adherence to institutional codes of conduct.
- **Monitor ongoing relationships:** Due diligence is not a one-time exercise. Institutions should periodically review third-party performance, conduct, and compliance with agreed standards. This might involve audits, feedback mechanisms, or data-sharing arrangements.
- **Respond to emerging risks:** Where concerns arise, whether through internal reports, external intelligence, or sector alerts, institutions should have protocols to reassess relationships and take appropriate action.

Due diligence records must show proportionate vetting aligned to the nature of the relationship, level of exposure, and current risk profile — with clear escalation procedures where concerns are identified[6].

5 Communication and Training

Institutions must ensure that all relevant individuals understand fraud risk and know how to act on concerns. A well-informed organisation is critical to early detection and confident response.

Effective communication and training help HEIs:

- **Deliver role-specific content:** Staff, contractors, and students encounter different risk scenarios. Messaging should reflect their context and equip them with actionable insights.
- **Use engaging formats and relatable examples:** Scenario-based training, real-life case studies, and plain-language policies help deepen understanding and encourage behavioural change.

- **Embed continuous learning:** Orientation programmes, refresher sessions, and campaign-based reminders ensure that fraud awareness remains fresh and embedded in institutional culture.

Training programmes should be aligned to identified risk areas and updated regularly. Attendance, feedback, and outcomes should be recorded to demonstrate procedural effectiveness and behavioural shift[7].

6 Monitoring and Review

Fraud prevention procedures must be actively maintained, reviewed, and refined. What works today may need improvement tomorrow.

Strong monitoring and review practices enable HEIs to:

- **Evaluate the effectiveness of controls over time:** Regular audits, peer reviews, and targeted inspections help validate and adjust institutional safeguards.
- **Link fraud oversight with governance mechanisms:** Integration into risk registers, committee structures, and performance dashboards ensures fraud resilience remains visible and accountable.
- **Learn from internal and external experience**: Institutions should actively reflect on incidents, both local and sector-wide, and use those lessons to enhance systems and culture.

Institutions should retain review records, demonstrate implementation of recommendations, and show how findings inform future planning — evidencing accountability and improvement[8].

Building Organisational Resilience

Resilience to financial crime in HEIs must be cultivated, it cannot be assumed. While policies and compliance frameworks offer a baseline, meaningful protection arises when institutions embed fraud awareness and ethical reflexes into their operational core.

A resilient HEI understands that fraud prevention is not the sole responsibility of Risk or Audit teams. It is a strategic function that spans leadership, frontline services, academic governance, and external engagement. Preventative measures must be proportional to the institution’s risk landscape, dynamically maintained, and transparently enforced.

Effective resilience begins with governance. Senior leaders should be engaged in fraud assurance reviews, not only to endorse prevention procedures but to challenge blind spots and support cultural change. Institutions must embed financial crime risk into enterprise risk management, ensuring clear visibility at board and committee levels.

Training is central to this effort. Generic compliance modules are no longer sufficient. Staff must be equipped to recognise manipulation tactics, red flag behaviours, and emerging typologies — such as refund fraud, synthetic identities, or misuse of student aid. Training should extend to those managing admissions, donor relations, and third-party partnerships.

Monitoring systems play an equally vital role. The use of analytics to detect anomalies, such as duplicated bank details, unusual payee patterns, or mismatches between academic and financial records, enables early intervention. In one recent case, student loan disbursements were used to fund travel to Syria for terrorist activity[9]. While rare, such incidents underscore the moral responsibility institutions hold in safeguarding legitimate funding streams.

Above all, resilience must be values-led. Ethical decision-making, transparency in incident response, and institutional learning from fraud events are hallmarks of mature organisations. Where incidents do occur, the focus should be on recovery, accountability, and building trust, not on reputational protection alone.

Sector-Specific Vulnerabilities and Risks

The Higher Education sector operates within a set of characteristics that make its exposure to financial crime distinct. Unlike many other industries, HEIs are tasked with balancing public service, commercial partnerships, academic autonomy, and international engagement, a multidimensional remit that creates pockets of vulnerability across their operations.

One major risk area lies in **franchised academic delivery**. HEIs often partner with external colleges and providers to deliver educational programs, particularly in overseas or vocational contexts. These partnerships, while economically advantageous, may be underpinned by inconsistent oversight or diluted accountability. The case involving the University of West London, where Oxford Business College submitted hundreds of fraudulent student loan applications, is a striking example of how misconduct at the periphery can ripple across institutional boundaries, undermining both trust and financial integrity[8].

Another significant exposure stems from **international recruitment and payment flows**. The global reach of UK HEIs is both a strength and a risk factor. The acceptance of tuition fees from third-party sources, sometimes via high-risk jurisdictions, opens the door to money laundering and financial manipulation. Cases presented at EnrolyCon 2025 revealed how some students had laundered millions in criminal proceeds through seemingly legitimate admissions and refund processes. These tactics exploit weak points in admissions due diligence and financial system monitoring, especially where payments are made by non-students or processed via manual intervention[9].

Donor and sponsorship relationships also require scrutiny. Many institutions rely on philanthropic contributions to fund research, scholarships, and capital projects. However, post-2022 investigations found that several leading UK universities had accepted funding from Russian-linked entities under sanctions or connected to politically exposed persons (PEPs). While not necessarily illegal at the time, such transactions present reputational, ethical, and compliance risks that demand proactive vetting.

Even students themselves can be part of the risk landscape. In recent cases, individuals were convicted for acting as **money mules**, transferring criminal funds through their personal accounts. These students were often unaware of the seriousness of their involvement or had been coerced via social engineering practices. HEIs must consider how student finance teams, welfare services, and campus security can collaborate to identify and respond to such patterns early.

While these risks reflect sector complexity, they do not signal institutional failure. With structured mitigation and informed leadership, HEIs can translate vulnerability into strengthened resilience[10].

Risk Monitoring and Internal Controls

Robust monitoring systems are the cornerstone of institutional fraud resilience. These mechanisms must be designed not only to detect anomalies but to embed learning and responsiveness across university operations.

HEIs should:

— **Extend monitoring beyond finance,** incorporating admissions, IT, advancement, and governance. This broader coverage reflects the interconnected nature of fraud risk across functional boundaries[13].

— **Invest in analytical tools** capable of flagging unusual transactional patterns, such as duplicate bank accounts, inconsistent payee data, or academic-financial discrepancies. These capabilities support early fraud detection and enhance investigatory capacity[11].

— **Link monitoring to governance structures,** ensuring escalation pathways feed into decision-making forums. This integration supports risk appetite calibration, accountability, and reputational protection[11].

— **Embed feedback loops** where monitoring results lead to realignment of training, controls, or risk thresholds. Resilience improves when institutions treat monitoring as a continuous improvement process, not a static compliance measure[11].

Data access and interpretation must also be governed by ethical principles, with due consideration given to privacy, proportionality, and the avoidance of profiling biases.

Managing Third-Party Relationships

Third-party relationships, from franchised academic delivery to international recruitment, represent a significant vector for financial crime exposure. Many recent sector incidents stemmed from insufficient oversight or unclear accountability across these partnerships[8, 9].

Key practices for institutions include:

— **Rigorous onboarding protocols:** Incorporating verification of corporate structure, financial integrity, and reputational standing[12].

— **Contractual clarity on fraud obligations:** Including cooperation in investigations, audit rights, and escalation procedures. Where third parties operate student-facing services, institutions must retain oversight and sanction powers[12].

— **Regular risk reviews:** Assessing conduct, performance metrics, and alignment with institutional values. These reviews should inform renewal decisions and governance reporting[12].

— **Strategic board-level visibility:** Recognising that third-party risk is a strategic exposure. Institutions must avoid siloed delegation or assumptions of external compliance[12].

The sector must also improve shared intelligence and horizon scanning, particularly as new models of global delivery and micro-credentialing emerge.

Safeguarding Students and Institutional Integrity

Students are increasingly exposed to financial crime threats, ranging from impersonation scams and coercive refund fraud to recruitment as money mules. HEIs have a moral and operational responsibility to protect students, not merely by ensuring secure transactions but by embedding fraud awareness into student support frameworks. Proactive education plays a foundational role; institutions should offer guidance on recognising social engineering, safe financial behaviours, and the risks associated with digital fraud. These efforts are best delivered through engaging campaigns, peer mentorship, and collaboration with external partners such as the NUS and law enforcement bodies[13].

In tandem, institutions must design financial workflows that prioritise security and detection. This includes verifying banking details, monitoring irregular payee activity, and integrating alerts into bursary and tuition processing systems. These safeguards should be reviewed regularly against evolving threat patterns, particularly in relation to vulnerable demographics and cross-border payments[13]. Responses to suspected fraud involving students must be empathetic and proportionate. Many participants in financial crime are manipulated or coerced, requiring institutions to involve welfare services and restorative approaches rather than defaulting to punitive action. By making student financial protection part of institutional duty of care, HEIs reinforce trust, resilience, and ethical accountability.

Embedding a Speak-Up Culture

The ability to detect financial crime early depends not only on systems but on people, and their confidence in being heard. A genuine speak-up culture requires more than policy statements; it demands visible, fair, and accessible channels through which staff and students can raise concerns. Institutions should offer a blend of reporting routes, including anonymous platforms, direct disclosures, and informal conversational options. Accessibility must account for varying comfort levels, languages, and roles, ensuring that no group is excluded from the reporting process[14].

Handling disclosures with integrity is equally critical. Reports must be managed confidentially and impartially, with clear feedback given to whistleblowers where appropriate. Institutional fairness — the assurance that raising a concern will not trigger retaliation or career harm — must be modelled consistently by leadership. Regular communications, case studies, and thematic reporting help to normalise the act of speaking up, moving it from compliance to cultural expectation. Ultimately, speak-up environments should be woven into the ethical identity of the institution, supporting not only fraud prevention but broader organisational integrity[14].

Towards a Fraud-Resilient HE Sector

Resilience against financial crime must extend beyond individual institutions; it is a shared ambition across the Higher Education sector. While universities differ in scale, funding models, and delivery, the underlying principles of fraud prevention are universally applicable. The introduction of the **Failure to Prevent Fraud** offence brings renewed emphasis to organisational accountability, demanding that HEIs take demonstrable action to deter, detect, and respond to criminal activity[2].

Building sector-wide resilience requires more than compliance. HEIs must integrate fraud governance into broader strategy and values frameworks, ensuring fraud prevention is treated not as a standalone risk but as part of institutional ethics, reputation, and trust. Collaboration is essential: institutions should exchange typologies, share tools, and co-create guidance to address emerging threats. Sector bodies, including Universities UK, Office for Students, and Universities and Colleges Information Systems Association, can play a catalytic role in curating shared intelligence, developing assurance standards, and disseminating good practice[5, 8].

Preparing for future risks also demands adaptive thinking. AI-enabled identity fraud, blockchain misuse, and manipulation of micro-credential ecosystems are not speculative, they are active threats requiring new controls and regulatory literacy. As institutions explore digital transformation, risk leaders must be embedded in innovation projects from the outset[5].

Above all, fraud resilience must be values-led. Institutions grounded in transparency, fairness, and organisational learning are better equipped to withstand reputational shocks and rebuild trust. The next frontier is not reactive policing, it is strategic foresight, ethical clarity, and operational maturity[17].

Conclusion

Financial crime presents an active and multifaceted threat to the UK Higher Education sector. From fraudulent student loan applications and donor vulnerabilities to weaknesses in financial workflows and oversight of third-party partners, HEIs must respond with strategic rigour and cultural integrity.

The enactment of the **Failure to Prevent Fraud** offence[2] signals a shift from passive compliance to demonstrable accountability. Institutions must take reasonable steps to deter, detect, and respond to fraud — embedding these obligations not only in their procedural frameworks but in their governance, values, and operational behaviours. Resilience is no longer a static concept; it must be dynamic, values-led, and integrated across every level of institutional activity[17].

This guidance has framed resilience through nine interconnected themes — from governance and monitoring to student safeguarding and sector-wide collaboration. Together, these themes underscore that resilience is not merely defensive; it is reputational, ethical, and foundational to public trust.

Next Steps for HEIs

Institutions should:

1. Review their existing fraud prevention frameworks against the new offence requirements[2].
2. Integrate fraud oversight into governance and enterprise risk reporting[3].
3. Ensure staff training reflects current typologies and includes frontline functions[9].

4. Strengthen monitoring across financial workflows and student interactions[11, 13].
5. Assess third-party relationship risks and update due diligence protocols[12].
6. Promote a speak-up culture with accessible and fair reporting mechanisms[14].

These actions collectively form a roadmap towards ethical leadership and fraud resilience in Higher Education.

By taking proactive, proportionate, and principled steps, HEIs can protect institutional resources, uphold sector credibility, and honour their educational mission. In doing so, they become not just compliant — but trusted, adaptive, and genuinely resilient.

References

1. HM Treasury. *Managing Public Money*. Annex 4.9: Fraud Risk Management. https://www.gov.uk/government/publications/managing-public-money
2. UK Government. *Economic Crime and Corporate Transparency Act 2023*, Section 199. https://www.legislation.gov.uk/ukpga/2023/56/section/199
3. National Audit Office. *Overcoming Challenges to Managing Risks in Government*. https://www.nao.org.uk/wp-content/uploads/2023/12/overcoming-challenges-to-managing-risks-in-government.pdf
4. Office for Students. *Preventing Fraud on Campus*. https://www.officeforstudents.org.uk/news-blog-and-events/blog/preventing-fraud-on-campus/
5. UK Finance. *Guidance on the Failure to Prevent Fraud Offence (ECCTA 2023)*. https://www.ukfinance.org.uk/policy-and-guidance/guidance/guidance-failure-prevent-fraud-offence-eccta-2023
6. Home Office. *Failure to Prevent Fraud Guidance*. https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta
7. Charity Commission. *Protecting Charities from Abuse for Extremist Purposes*. https://www.gov.uk/government/publications/protecting-charities-from-abuse-for-extremist-purposes
8. Office for Students. *Condition E3: Accountability*. https://www.officeforstudents.org.uk/publications/regulatory-framework-for-higher-education-in-england/part-v-guidance-on-the-general-ongoing-conditions-of-registration/condition-e3-accountability/
9. Diligent. *Preventing Higher Education Fraud with Audit and Risk Collaboration*. https://www.diligent.com/resources/blog/new-era-fraud-higher-education
10. Pinsent Masons. *UK Higher Education Institutions Must Be Alert to Suspicious Financial Activity*. https://www.pinsentmasons.com/en-gb/out-law/news/uk-higher-education-suspicious-financial-activity-alert
11. University of Reading. *Universities and Their Students Are Vulnerable to Money Laundering*. https://research.reading.ac.uk/research-blog/2023/09/18/universities-and-their-students-are-vulnerable-to-money-laundering-new-research/
12. Browne Jacobson. *How Universities Can Navigate the New 'Failure to Prevent Fraud' Offence*. https://www.brownejacobson.com/insights/how-universities-can-navigate-the-new-failure-to-prevent-fraud-offence
13. UK Finance & Cifas. *Don't Be Fooled Campaign – Student Financial Safety Resources*. https://www.dontbefooled.org.uk
14. Protect (formerly Public Concern at Work). *Whistleblowing Advice and Guidance*. https://protect-advice.org.uk

Further Reading

1. National Crime Agency – *Suspicious Activity Reports and Financial Intelligence* https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports
2. Universities UK (UUK) – *Security and Risk Guidance for Higher Education Institutions* https://www.universitiesuk.ac.uk/topics/funding-finance-and-operations/security-and-risk
3. Charity Commission – *Protecting Charities from Harm: Compliance Toolkit* https://www.gov.uk/government/collections/protecting-charities-from-harm-compliance-toolkit
4. UCISA – *Cyber Security Frameworks and Sector Benchmarks* https://www.ucisa.ac.uk/-/media/A085D01694C849529E163CE9C0DC4E82.ashx
5. Public Sector Fraud Authority (PSFA) – *Standard for Fraud Detection Practitioners* https://www.gov.uk/government/publications/practitioners-standard-for-fraud-detection/psfa-standards-standard-for-fraud-detection-practitioners-html

6. OECD – *Health at a Glance 2023: Avoidable Hospital Admissions and System Resilience* https://www.oecd.org/en/publications/health-at-a-glance-2023_7a7afb35-en/full-report/avoidable-hospital-admissions_836e2826.html

7. Financial Times FLIC. *Financial Literacy and Inclusion Campaign*.
https://ftflic.com

8. Universities UK. *Tackling Harms in International Student Recruitment*.
https://www.universitiesuk.ac.uk

9. UCISA. *Cyber Security and Resilience in Higher Education*.
https://www.ucisa.ac.uk

Further information

For access to further RMP Resources you may find helpful in reducing your institution's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your broker, RMP risk control consultant or account director.

contact@rmpartners.co.uk

Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

This document does not purport to be comprehensive or to give legal advice. While every effort has been made to ensure accuracy, Risk Management Partners cannot be held liable for any errors, omissions or inaccuracies contained within the document. Readers should not act upon (or refrain from acting upon) information in this document without first taking further specialist or professional advice.

Risk Management Partners Limited is authorised and regulated by the Financial Conduct Authority. Registered office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company no. 2989025.