INDEPENDENT HIGHER EDUCATION AUSTRALIA

IHEA SUBMISSION

HIGHER EDUCATION STANDARDS COMMITTEE CONSULTATION PAPER: STRENGTHENING RESEARCH SECURITY AND NATIONAL SECURITY EXPECTATIONS IN THE HIGHER EDUCATION STANDARDS FRAMEWORK

7 September 2026

IHEA Submission

Higher Education Standards Committee Consultation Paper: Strengthening Research Security and National Security expectations in the Higher Education Standards Framework (Threshold Standards)

Independent Higher Education Australia (IHEA) welcomes the opportunity to provide input to the Higher Education Standards Committee Consultation Paper: Strengthening Research Security and National Security expectations in the Higher Education Standards Framework (Threshold Standards), for which submissions are due by 7 September 2026.

Introduction

The Consultation Paper is seeking views to inform advice on whether, and if so how, research security and national security governance expectations should be reflected in the Threshold Standards.

However, it does not set out specific proposed amendments for consultation. As such, any future amendments to the Threshold Standards should be released as specific proposals for consultation.

As a matter of good practice, if the Higher Education Standards Committee (HESC) or the Australian Tertiary Education Commission (ATEC) propose amendments to the Threshold Standards, stakeholders should have an opportunity to review and comment on the actual proposed drafting, including its scope, application, proportionality and implementation, before any changes are finalised.

IHEA considers that any changes to the Threshold Standards should build on the existing principles–based and outcomes–focused framework to apply a proportionate, risk based approach to cyber security, research security and national security risks. The existing Threshold Standards already provide a substantive foundation for providers to identify, manage and provide assurance over risks relevant to these areas.

For example:

- **Standard 7.3.3(b)** requires providers to maintain information systems and records securely and confidentially, including protection against unauthorised or fraudulent access to private or sensitive information.
- **Section 4.1 (Research)** establishes requirements relating to research.
- **Section 5.2 (Academic and Research Integrity)** establishes requirements relating to academic and research integrity.
- **Section 5.4 (Delivery with Other Parties)** is relevant to the provider's accountability for activities undertaken through other/third parties.
- **Section 6.2 (Corporate Monitoring and Accountability)** and **Section 6.3 (Academic Governance)** establish requirements concerning institutional monitoring, accountability and governance, including oversight of risk management, compliance and academic governance.

Together, these provisions provide an existing framework through which relevant cyber security, research security and national security risks can be identified, managed and subject to appropriate assurance. The focus should therefore be on ensuring that these existing requirements are applied consistently and proportionately, rather than assuming that new prescriptive requirements are necessary.

Any regulatory response should also recognise the diversity of Australia's higher education sector and the significant differences between providers in size, mission, research activity, information holdings, digital infrastructure, institutional complexity and risk exposure. The nature and level of security risks, and the controls reasonably required to address them, will therefore differ between providers.

IHEA's preferred approach is to address the issues through the existing Threshold Standards, supported by a Tertiary Education Quality and Standards Agency (TEQSA) Statement of Regulatory Expectations (SRE) and appropriate provider specific guidance. This would provide greater clarity about how existing requirements are expected to be interpreted and assured without adding new requirements to the Standards.

An SRE and appropriate guidance would clarify how existing Standards apply to different categories of security risk, while allowing regulatory expectations and assurance activities to be differentiated according to provider circumstances and risk profile.

This would strengthen clarity and consistency, avoid unnecessary duplication and reduce the risk that expectations developed for higher risk institutions are indiscriminately applied to providers with materially different and lower levels of risk exposure.

The Consultation Paper distinguishes between cyber security risks, which can arise across providers irrespective of research intensity, and research security risks, which vary according to the nature, scale and sensitivity of research activity. Any regulatory response should preserve that distinction and ensure that requirements are proportionate to actual risk rather than applied uniformly on the basis of provider category or institution type.

This issue is also directly relevant to the House Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations, which was established on 4 June 2026. The Committee is examining, among other matters, the adequacy and accessibility of government cyber security guidance, the appropriateness of standards for small and medium sized organisations, access to cyber security services and employee training.

IHEA considers that these matters reinforce the importance of supporting organisations through practical, accessible guidance, rather than responding to each specific cyber security issue through additional bespoke regulatory requirements.

IHEA is also concerned about the growing regulatory burden on providers arising from an approach of developing bespoke regulatory requirements to address each specific issue, rather than building on performance based regulation and supplementing it with clear, practical guidance.

Each additional requirement can add compliance obligations, processes and evidence requirements, increasing regulatory complexity even where the underlying objective could be achieved through existing standards and regulatory tools. This is particularly relevant for smaller providers, which may have fewer resources and less specialist capability to manage multiple overlapping regulatory requirements.

Recommendations

1. **Use existing regulatory tools before amending the Standards:** HESC and ATEC should consider addressing the issues raised in the Consultation Paper through the existing Threshold Standards, supported where appropriate by a TEQSA SRE and guidance. If amendments are ultimately proposed, the specific drafting should be released for further consultation before it is settled.
2. **Retain the principles–based and outcomes–focused approach of the Threshold Standards:** The Standards should establish the outcomes and institutional responsibilities providers must achieve, rather than prescribe particular structures, registers, reporting systems, technologies or processes for achieving them.
3. **Apply cyber security expectations across the sector, but proportionately:** Providers should protect their information, systems and operational infrastructure in a manner commensurate with their circumstances and risk profile. The nature and sophistication of the controls should reflect factors including the provider's size, systems, information holdings, digital dependency, institutional complexity and overall risk exposure.
4. **Differentiate research security expectations according to actual research activity:** Research security expectations should apply where a provider's research or related activities create relevant risks, with the

nature and extent of those expectations reflecting the nature, scale, sensitivity and risk profile of the provider's actual research activities.

5. **Recognise differences in research intensity across provider categories:** The Australian University category has specific research requirements under Part B of the Threshold Standards, including B1.3.16–19. However, Table B universities and NUHEPs should not be assumed to have the same research security risk profile as the most research–intensive Table A universities. More detailed requirements may be appropriate where a provider undertakes substantial or higher risk research, but should reflect its actual research activity, capability, partnerships, information and intellectual property holdings and associated risks.
6. **Avoid duplication with existing frameworks:** The Threshold Standards and any supporting regulatory expectations should complement, rather than reproduce, existing legislative, funding and sector frameworks, including the University Foreign Interference Taskforce (UFIT) Guidelines, ARC research security requirements, sanctions, export controls and other applicable national security obligations.

Use the Existing Threshold Standards, Supported by an SRE and Provider Specific Guidance

IHEA's preferred approach is to build on the existing Threshold Standards. The Consultation Paper itself identifies a number of existing provisions that are relevant to cyber security, research security and national security risks. Where an existing Standard already establishes the relevant outcome, the more proportionate response may be to clarify how that outcome is expected to be achieved and assured.

The existing Standards establish relevant institutional responsibilities. As identified in the Consultation Paper, these include Standard 7.3.3(b), Standards 4.1.1, 5.2.2, 5.2.4 and 5.4.2, and Sections 6.2 and 6.3. These provisions address matters including secure information systems and records, governance, research partnerships, research integrity and critical incidents. IHEA considers that these existing requirements should be used as the starting point for any further regulatory response.

IHEA therefore recommends that a TEQSA SRE and supporting guidance would provide the additional clarity needed to apply and assure the existing Threshold Standards in relation to cyber security, research security and relevant national security risks.

An SRE could explain how TEQSA expects the existing Threshold Standards to be interpreted and assured in relation to these risks. It could, for example:

- Identify the existing Threshold Standards relevant to these risks.
- Explain the outcomes providers are expected to achieve.
- Clarify the circumstances in which particular risks may warrant greater attention.
- Explain how proportionality will be applied.
- Identify relevant existing legislative, funding and sector obligations.
- Make clear where those external obligations apply only to particular providers, research activities or funding arrangements.
- Provide transparency about the evidence that may reasonably be expected to demonstrate that the relevant outcomes have been achieved.

The SRE should not purport to amend the Threshold Standards or create requirements that are inconsistent with them. It should clearly distinguish between the obligations established by the Standards and TEQSA's regulatory expectations concerning how providers may demonstrate that those obligations have been met.

The SRE should be supported by provider specific guidance explaining how providers with different characteristics might appropriately achieve the relevant outcomes. Guidance should take account of provider category and institutional role; size and organisational complexity; the nature, scale and maturity of research activity; the sensitivity of information and intellectual property held; reliance on digital systems; research partnerships and international collaborations; and the provider's particular risk profile.

This approach recognises that the same outcome may be achieved through different systems, controls and governance arrangements, reflecting differences in provider size, activities and risk profile.

Guidance should be clearly identified as guidance and should not become a de facto source of additional mandatory requirements. It should provide examples of proportionate approaches rather than establish a single prescribed compliance model. Guidance should not purport to amend or materially expand the requirements established by the Threshold Standards.

An SRE and supporting guidance could also allow regulatory expectations to evolve as risks and technologies change without requiring repeated amendments to the Threshold Standards. This approach would allow regulatory expectations to evolve as risks change while preserving greater stability within the Threshold Standards themselves.

Proportionate Application of Cyber Security and Research Security

Cyber security and research security are related but distinct issues and should not be assumed to require the same regulatory response. The distinction is important because cyber security risks may arise across the sector, whereas research security risks depend more directly on the nature, scale and sensitivity of research activity.

Cyber Security

Cyber security expectations may be relevant across the higher education sector. All providers rely on information systems and hold sensitive information, including personal, student, staff and institutional data that must be appropriately protected.

The Consultation Paper recognises that cyber security risks can arise regardless of the scale or intensity of a provider's research activity. It identifies risks associated with sensitive information, research systems, proprietary knowledge and other information assets, and acknowledges that the consequences of a cyber incident may be significant even for providers with limited research activity.

While the Consultation Paper proposes that cyber security should be considered across the sector, it does not propose any specific amendments to the Threshold Standards. If specific cyber security controls, assurance requirements or evidentiary expectations are proposed in the future, they should be the subject of further consultation with stakeholders.

However, providers should not be expected to satisfy identical cyber security requirements. The appropriate regulatory outcome is for providers to maintain cyber security governance arrangements and security controls that are fit for purpose and proportionate to their size, operating environment and risk profile.

For a small, teaching focused provider, this may involve protecting student and staff information, learning management systems, financial systems and other administrative systems. Providers with more extensive research activity, significant research infrastructure or large volumes of sensitive research data may reasonably require more sophisticated cyber security arrangements.

Different operating models should not be interpreted as evidence of weaker cyber security. Providers may achieve comparable outcomes through different governance arrangements, outsourced expertise and technology environments

An SRE and accompanying provider guidance should clearly explain these different expectations while avoiding a one–size–fits–all approach to cyber security.

Research Security

Research security risks may arise from matters including sensitive research data and intellectual property, research partnerships and collaborations, international engagement, dual–use technologies, research infrastructure and other activities with potential national security implications.

In principle, the general risk–based proposition in the Consultation Paper is appropriate but it does not yet identify specific research security requirements that providers would be expected to meet. Any detailed requirements should therefore be assessed against the actual proposed drafting, including their necessity, proportionality, regulatory burden and interaction with existing obligations.

Research security is more closely connected to the nature and extent of research activity undertaken by a provider. Risks may arise from matters including sensitive research data and intellectual property, research partnerships and collaborations, international engagement, technologies that have both civilian and potential military or security applications, research infrastructure and other activities with potential national security implications. Research security expectations should therefore reflect the actual activities and risks of each provider.

The Australian University category has a distinctive research role, with specific research requirements under Part

B, including B1.3.16–19 of the Threshold Standards. The Consultation Paper raises, but does not propose, the possibility of using Part B for more specific research security requirements. If that option is pursued, the specific proposed requirements and drafting should be subject to further consultation so that providers can assess their scope, application and regulatory impact.

Not all universities, however, have the same research security risk profile. Table A and Table B status may be relevant contextual information but should not substitute for an assessment of actual research activity and associated risk. Some Table B providers may undertake significant research, while others may be predominantly teaching–focused. Other higher education providers may also undertake research or research training at different scales.

Provider category can therefore inform the assessment of risk, but the nature, scale and associated risks of a provider's actual research activity should determine the nature and extent of research security expectations.

Requirements designed for the most research intensive universities should not be applied indiscriminately to Table B universities or NUHEPs whose research activities do not present equivalent risks. If more specific requirements are proposed, they should be calibrated to the actual research activities, capability, partnerships, information and intellectual property holdings and associated risks of the provider.

The appropriate regulatory principle is that research security obligations should be proportionate to the nature, scale and risk profile of the research and related activities undertaken by the provider. Provider category may inform the application of these obligations, but should not, in itself, determine the requirements that apply.

Responses to the HESC Consultation Questions

Question 1 – Assurance Mechanisms and Support for Staff and Research Students: How might current assurance mechanisms be strengthened to support providers identify, assess, manage and mitigate research security, cyber security and national security risks, while appropriately supporting and protecting staff and research students and other university affiliated or visiting staff engaged in those activities?

IHEA Response

IHEA considers that current assurance mechanisms can be strengthened principally through clearer regulatory expectations and provider–specific guidance applied against the existing Threshold Standards. Because the Consultation Paper does not set out specific amendments, IHEA considers that any assessment of particular regulatory requirements should await the release of actual proposed drafting.

For providers with limited or no material research activity, existing governance, risk management and information management requirements should provide the principal assurance mechanism. Standard 7.3.3 already contains requirements concerning the secure management of information systems and records. Cyber security assurance should focus on protecting the provider's information, systems and operational infrastructure in a manner proportionate to its circumstances.

Where a provider undertakes material research activity, its assurance arrangements should be proportionate to the nature, scale and sensitivity of the research activity being undertaken. Providers should be able to demonstrate that they have identified and managed reasonably foreseeable risks associated with their research activities, including, where relevant, research data, intellectual property, partnerships, international collaboration and research infrastructure.

For Australian Universities and other providers undertaking substantial or higher–risk research activity, more sophisticated governance and assurance arrangements may be appropriate. IHEA does not support a universal requirement for every provider to establish dedicated national security functions, specialist research security structures or complex research security registers irrespective of its activities and risk profile.

A TEQSA SRE and provider–specific guidance could allow expectations to be differentiated while maintaining a consistent regulatory outcome and supporting staff and researchers through proportionate training, guidance and

assurance arrangements.

Question 2 – Alignment with Existing Frameworks and Avoiding Duplication: Are there existing legislative, regulatory, funding or sector frameworks, including ARC funding requirements, UFIT, national security obligations and other research governance mechanisms, that should be taken into account in developing any new or clarified expectations? If so, how should those expectations be framed to avoid unnecessary duplication and support effective implementation?

IHEA Response

The existing national security and research governance framework is extensive. The Consultation Paper identifies, among other mechanisms, the Foreign Relations (State and Territory Arrangements) Act 2020, Australian sanctions legislation, the Defence Trade Controls Act 2012, the Security of Critical Infrastructure Act 2018, ARC research security requirements and the UFIT Guidelines. Any Threshold Standards requirements should operate as a complementary institutional governance framework rather than reproduce the detailed requirements of those regimes.

The Threshold Standards should complement, rather than reproduce, duplicate or overlap with the detailed requirements of those regimes. Specialist legislation, funding conditions and sector frameworks are generally better placed to establish detailed technical or activity–specific requirements.

The UFIT Guidelines should remain appropriately targeted to the university sector and should not be converted through Part A into a detailed mandatory framework applying to all higher education providers. The Consultation Paper recognises UFIT as a voluntary framework and indicates that any Threshold Standards expectations should complement rather than duplicate it.

ARC research security requirements should likewise remain connected to the research and funding activities to which they apply. The Consultation Paper notes that the ARC Research Security Framework is directed to ARC–funded research and sits alongside other mechanisms, and that not all research undertaken by registered higher education providers is funded through ARC or NHMRC programs. Any Threshold Standards requirements should therefore establish appropriate institution–wide governance without duplicating ARC–specific requirements.

Detailed obligations arising under sanctions, export controls, foreign arrangements or other specialist national security legislation should likewise not be replicated in the Threshold Standards. Providers should instead have governance arrangements appropriate to their activities to identify and manage the obligations that apply to them.

A TEQSA SRE and supporting guidance could help explain the relationship between the Threshold Standards and these existing obligations, including where particular obligations apply only to particular providers, research activities or funding arrangements. This would improve clarity without creating unnecessary duplication.

Question 3 – Implementation Challenges, Risks and Unintended Consequences: What implementation challenges, risks or unintended consequences should HESC consider in developing advice on potential amendments to the Threshold Standards, and what measures could support effective, proportionate and risk based implementation across the sector?

IHEA Response

The principal implementation risk is that broad national security objectives could result in prescriptive and disproportionate regulatory requirements being applied to providers whose activities do not present equivalent risks. This risk is particularly relevant because the Consultation Paper does not yet set out the specific requirements that might be imposed.

Independent higher education providers vary considerably in size, organisational complexity, research activity and access to specialist resources. Many are predominantly teaching–focused and operate with comparatively lean

governance and administrative structures. Requirements designed around the governance structures and research environments of large research–intensive universities could therefore impose significant compliance costs without a corresponding increase in national security outcomes.

The Consultation Paper recognises that additional governance, reporting, training and assurance requirements may impose direct and indirect costs and that regulatory change should balance security objectives with proportionality, institutional agility, openness and collaboration. These principles should guide the assessment of any specific amendments that may subsequently be proposed.

IHEA recommends that any new or clarified expectations take explicit account of provider category; the nature, scale and maturity of research activity; the type and sensitivity of research data, intellectual property and infrastructure; international research and collaboration activities; and the actual national security, cyber security and research security risks associated with those activities.

Provider category should inform the risk assessment but should not determine the outcome. Australian Universities may require more detailed research security expectations where justified by their activities and the existing research requirements in Part B. Table B providers and other research–active providers should be subject to requirements proportionate to their actual research activities and risk exposure, while providers with limited or no material research activity should not be required to establish research security governance arrangements designed for research–intensive universities.

The Threshold Standards should specify the outcomes providers are expected to achieve while allowing providers to determine the systems, policies and processes appropriate to their circumstances. This is particularly important for smaller providers, which may achieve equivalent security outcomes through simpler governance arrangements, external expertise, managed services or shared specialist capability.

Providers should not be required to establish dedicated national security governance structures, specialist research security functions, complex risk registers or other specialised arrangements where these are not justified by their activities or risk profile. The Standards should allow providers to meet the required outcomes through governance arrangements appropriate to their size and circumstances.

Regulatory expectations should therefore focus on whether the required outcomes are effectively achieved and assured, rather than whether a provider has adopted a particular organisational model or set of controls.

If amendments are ultimately proposed, HESC, ATEC and TEQSA should support implementation through clear guidance, practical examples for different provider profiles, templates and tools where appropriate, opportunities for provider education and engagement, and an appropriate transition period before new requirements are subject to regulatory assessment. Any guidance should make clear that examples are illustrative and do not constitute additional mandatory requirements beyond the Threshold Standards.

Furthermore, frequent changes to regulatory expectations can create significant implementation costs for smaller providers that are already managing multiple compliance, reporting and funding obligations.

TEQSA's implementation should also take account of existing legislative, funding and policy obligations. Providers should not be required to demonstrate compliance separately against multiple substantially equivalent frameworks where evidence of compliance with one framework can reasonably provide assurance for another.

Conclusion

IHEA's position is that any regulatory response should recognise that Australia's higher education sector is diverse and that the nature, scale and risk profile of research and cyber security exposure varies between providers.

As such, IHEA's preferred approach is to make better use of the existing Threshold Standards, supported where appropriate by a TEQSA Statement of Regulatory Expectations and guidance. This would provide greater regulatory clarity and consistency while allowing expectations to be differentiated according to provider circumstances and risk, without unnecessarily expanding the Threshold Standards.

However, if, following this consultation, further amendments are considered necessary, the specific proposed drafting should be the subject of a further consultation process.

Research security expectations should be calibrated to the provider's actual research activities and associated risks. Table B universities and NUHEPs should not be assumed to have the research profile or risk exposure of the most research–intensive Table A universities. If more specific requirements are proposed, they should be assessed against the actual activities and risks of the providers to which they would apply.

The central principle should be that research security obligations are proportionate to the nature, scale and risk profile of the research and related activities undertaken by the provider, with provider category informing—but not determining—the appropriate requirements. Cyber security expectations may appropriately apply across all providers but should likewise be proportionate to institutional circumstances and risk.

This approach would strengthen research security and national resilience while preserving the differentiated intent of the Threshold Standards, minimising unnecessary regulatory burden and directing regulatory effort towards areas of genuine and material risk. It would also ensure that stakeholders are able to assess and comment on the actual regulatory requirements before they are finalised.

Who We Are

Independent Higher Education Australia Ltd. (IHEA) is a peak body established in 2001 to represent Australian independent (private sector) higher education institutions. Our membership spans independent universities, university colleges and other institutes of higher education, all of which are registered higher education providers accredited by the national higher education regulator, TEQSA or associate members seeking registration.

There is a long tradition of independent higher education providers in Australia, with the first provider created as early as 1815, only 27 years after the first British settlement in Sydney in 1788. In total, five providers were established between 1815 and 1845 and preceding the first public university. The fifth of these was St James College, which was created in 1845. The founders of St James College were then involved in creating Moore College in 1856 and remarkably Moore College, a University College, still exists and is Australia's longest continuously operating independent higher education provider.

Our Vision is that: students, domestic and international, have open and equitable access to world class independent higher education in Australia, built on the foundations of equity, choice and diversity.

Our Mission is to represent independent higher education and promote recognition and respect of independent providers as they contribute to Australian education, the Australian economy and to society in general. We achieve this by promoting continuous improvement of academic and quality standards within member institutions, by advocating equity for their staff and students and by delivering services that further strengthen independent providers' reputations as innovative, sustainable and responsive to the needs of industry and other relevant stakeholders in both higher education and vocational education and training. IHEA's commitment is to excellence, productivity and growth in independent higher education being delivered through a trusted Australian education system underpinned by equity, choice and diversity.

IHEA members have different missions, scales and course offerings across the full AQF range (Diplomas to Doctorates). IHEA has 94 members, which rises to over 120 if providers' constituent colleges and subsidiaries are included.

IHEA's 94 members comprise:

- Five private Universities (Australian University of Theology, Avondale University, Bond University, Torrens University and University of Divinity).
- Six University Colleges (ACAP University College, Australian University College of Divinity, Alphacrucis University College, Excelsia University College, Moore Theological College and SAE University College).
- Eighty not–for–profit and for–profit institutions of higher education (which includes twelve full or partially self–accrediting institutes); and related corporate entities.
- Three corporate owners of higher education providers.

IHEA members teach approximately 74 percent of the students in the independent sector (i.e., more than 140,000 students) and educate students in a range of disciplines, including law, agricultural science, architecture, business, accounting, tourism and hospitality, education, health sciences, theology, creative arts, information technology, human services and social sciences.

IHEA holds a unique position in higher education as a representative peak body of higher education providers. Membership in IHEA is only open to providers registered, or seeking registration, with the Australian regulator – TEQSA. However, some IHEA members are dual and multi–ϖsector providers who also deliver VET and/or English Language Intensive Courses for Overseas Students (ELICOS) courses.

Contacts:

The Hon. Dr. Peter Hendy
Chief Executive Officer
Email: Peter.Hendy@ihea.edu.au
Phone: 0418 679 911

Dr James Hart
Chief of Policy
Email: James.Hart@ihea.edu.au
Phone: 0418 694 680

IHEA Member Institutions

Universities

- Australian University of Theology
- Avondale University
- Bond University
- Torrens University Australia
- University of Divinity

University Colleges

- ACAP University College
- Alphacrucis University College
- Australian University College of Divinity
- Excelsia University College
- Moore Theological College
- SAE University College

Institutes of Higher Education

- Academies Australasia Polytechnic
- Academy of Interactive Technology
- Acknowledge Education
- Adelaide Central School of Art
- AIBI Higher Education
- AIM Business School
- Australasian Academy of Higher Education
- Australasian College of Health and Wellness
- Australian Chiropractic College
- Australian College of Christian Studies
- Australian College of Nursing
- The Australian College of Physical Education
- Australian Data and Cyber Institute
- The Australian Institute of Music
- Barton Business School
- Campion College Australia
- Central Institute of Technology and Innovation
- Christian Heritage College
- CIHE Australia
- COLLARTS
- The College of Law
- Eastern College Australia
- Education Centre of Australia
  - Asia Pacific International College
  - ECA College of Health Sciences
  - Higher Education Leadership Institute
- Endeavour College of Natural Health
- EQUALS International
- Fairmont College Australia
- Gateway Business College
- Governance Institute of Australia
- Holmes Institute
- IBC Education
- iCareers Institute
- ICHM
- Ikon Institute of Australia
- International College of Management, Sydney
- International School of Global Leaders
- JMC Academy
- Kaplan Business School
- Kaplan Higher Education
- King's Own Institute
- Laurus Higher Education
- LCI Melbourne
- Le Cordon Bleu Australia
- Leaders Institute
- Lyons College
- Marcus Oldham College
- MIECAT
- Morling College
- Nan Tien Institute
- National Institute of Organisation Dynamics Australia
- Navitas
  - Curtin College
  - Edith Cowan College
  - Eynesbury College
  - Deakin College
  - La Trobe College Australia
  - Griffith College
  - SAIBT
  - SIBT
  - Western Sydney University International College
- Nova Higher Education
- Ozford Institute of Higher Education
- Photography Studies College
- Polytechnic Institute Australia
- Russo Business School
- Sheridan Institute of Higher Education
- Skyline Higher Education Australia
- S P Jain School of Global Management
- Stanley College
- Sydney Institute of Higher Education
- Sydney International School of Technology and Commerce
- Sydney Met
- Southern Academy of Higher Education
- Tabor College
- The Tax Institute Higher Education
- Torrens University Australia
  - Think: Colleges
- Universal Business School Sydney
- Universal Higher Education
- UoW College
- UTS College
- Wentworth Institute

Economic contribution of independent higher education

IHEA INDEPENDENT HIGHER EDUCATION AUSTRALIA

NineSquared

Key Findings.

Independent higher education is an important contributor to Australia's economic activity.

The sector contributes

$8.2 billion

to Australia's GDP

For every **$3** the sector directly contributes to GDP, it supports around **$1** of additional value added elsewhere in the economy

International students contribute

$7.6 billion

to Australia's GDP

Supports

18,906 FTEs

across the economy

196,000 students

61% International*

39% Domestic*

*Shares based on EFTSL

Contributes

$3.0 billion

in government tax revenue

Increases output by

$14.0 billion

Contributes

$13.1 billion

to total incomes

The sector contributes to the Australian economy through several major impact channels:

- institutional spending
- international student living expenses
- expenditure of visiting friends and family
- net increase in student labour supply
- graduate labour productivity uplift
- research driven productivity uplift