Management and accountability

Risk management

In 2024, UTS further enhanced its enterprise risk management framework, which aligns with international standards (ISO 31000:2018, Risk Management — Guidelines). This framework continues to support all aspects of university operations, including academic activities, research, change initiatives, financial planning and legal compliance.

Building on the progress made in 2023, UTS has strengthened its risk maturity by adapting to evolving operational and external risk landscapes. Through a continued focus on fostering a risk-aware culture, the university has improved decision-making processes, enhanced asset protection and reinforced stakeholder confidence.

In 2024, all staff members at UTS continue to play a vital role in risk management, ensuring that risks are identified, assessed and managed within the university's defined risk appetite. By fostering a culture of informed risk-taking, UTS has strengthened its ability to navigate challenges and drive innovation and sustainable growth and success.

UTS continued to advance its enterprise risk management framework this year by building on improvements made in 2023. Key enhancements include:

- expanded periodic external threat landscape scans to proactively identify emerging risks and strengthen resilience
- refined the risk taxonomy to cover strategic, operational, academic and compliance risks
- further strengthened risk governance with clear roles and responsibilities of UTS Council and its committees and the University Leadership Team in risk oversight and monitoring effectiveness of risk mitigation strategies
- increased on-the-job training of staff on risk management during periodic risk and opportunity review processes.

In 2024, UTS further advanced its synergistic approach to integrate insurance as a financial protection against risks. This allowed UTS to strengthen risk mitigation strategies that balance prevention, control and financial protection for risks that cannot be fully mitigated.

UTS maintains a comprehensive insurance program to cover the university and its controlled entities. These include:

- financial lines (including directors and officers, cyber, medical malpractice, commercial crime, professional indemnity, employment practices liability)
- public, products and environmental liabilities
- property and asset protection and business interruption
- accident and health (including travel insurance)
- staff and students international health and security management through International SOS.

Academic Freedom and Freedom of Expression Attestation Statement

This annual statement attests that the UTS Council is satisfied that the university:

- has a policy that upholds academic freedom and freedom of expression as paramount values, as required under the Model Code
- maintains an institutional environment in which academic freedom and freedom of expression are upheld and protected
- addresses questions in relation to the management of academic freedom and freedom of expression issues promptly, actively and in good faith.

UTS respects and promotes academic freedom and freedom of expression primarily through its Academic Freedom and Freedom of Expression Policy (and supported by commitments outlined in other university-wide policies) and its enterprise agreements. The Academic Freedom and Freedom of Expression Policy makes clear UTS's position to uphold academic freedom and freedom of expression as paramount values that meet the requirements of the Model Code.

In an environment of heightened tensions in the Middle East, and considering the impacts on our local community, in 2024 UTS took a range of measures to ensure the safety and wellbeing of our community, while supporting the right for students and staff to express their opinions and contribute to public debate.

Over the last 12 months UTS has reviewed its governance settings to better manage safety in the context of protests and demonstrations and clearly articulated its expectations of staff, students and the broader university community. In providing this statement of attestation, UTS reiterates its commitment to academic freedom and freedom of expression, while safeguarding student and staff wellbeing.

Statement on Voluntary Code of Best Practice for the Governance of Australian Public Universities

The Voluntary Code of Best Practice for the Governance of Australian Public Universities provides a framework to assess performance and to ensure transparency and accountability in a university's governance arrangements. It contains 14 protocols, each of which have several sub-components. For protocol 12(b), regarding the independence of controlled entity board directors, UTS has chosen in some instances to not adhere to the protocol's requirements. This approach has been the case since the code's adoption.

In 2024, UTS was fully compliant with 13 of the code's protocols and, noting the above exception, partially compliant with the remaining protocol. The university reviews its compliance on an annual basis.

Statement on Voluntary Code of Australian Universities Vice-Chancellor and Senior Staff Remuneration Code

The Australian Universities Vice-Chancellor and Senior Staff Remuneration Code is a voluntary set of principles and processes designed to ensure fair and appropriate remuneration for university leadership that is understood and supported by the sector.

UTS acknowledges the importance of ensuring the remuneration of its Vice-Chancellor and senior leaders is competitive, appropriate and transparent.

Remuneration needs to appropriately reflect the value that high quality leaders bring to the university, and the broader economy and society, while also acknowledging the role of universities as public purpose institutions.

Transparency is a vital part of good practice remuneration ensuring that decision-making bodies, processes and outcomes are openly explained and readily available to all stakeholders.

UTS has a Remuneration Committee comprising the Chancellor, Deputy Chancellor and one Council-appointed person whose term of appointment is not about to expire. The committee advises Council on the Vice-Chancellor's and Provost's performance and remuneration. In addition to the Remuneration Committee of Council, UTS also has a Vice-Chancellor's Remuneration Committee that considers senior executive management performance and remuneration.

The Remuneration Committee of Council and the Vice-Chancellor's Remuneration Committee meet biannually to review remuneration: once to determine variable performance pay outcomes and once for annual remuneration setting.

In determining performance pay outcomes, each committee considers institutional and individual performance. Institutional performance is reviewed against the UTS corporate plan and annual KPI scorecard, which includes a range of financial and non-financial targets. Individual performance reviews are required to be undertaken annually and consider individual performance from a leadership, culture and risk management perspective. Recommendations are submitted to the relevant committee for determination and approval.

In setting remuneration, an annual remuneration review is completed for the Vice-Chancellor, the Provost and senior executive management to ensure remuneration is competitive from an attraction and retention perspective and within range in comparison to higher education sector relativities. Sector remuneration and benefit benchmark data for comparable roles as well as market observations and movements are provided to the relevant committee for determination and approval.

Senior executive remuneration

Band	2023		2024	
	Female	Male	Female	Male
Band 4 (Vice Chancellor)	–	1	–	1
Band 3 (Provost)	1	–	1	–
Band 3 (Deputy Vice-Chancellor)	2	2	3	1
Band 3 (Chief Operating Officer)	–	1	–	1
Total	**3**	**4**	**4**	**3**

Band[1]	Range	2023	2024
Band 4 (Vice-Chancellor)	$900,000–$999,999	1	1
Band 3 (Provost, Deputy Vice-Chancellor and Chief Operating Officer)	$500,000–$699,999	6	6
Total		**7**	**7**

1. Bands are reflective of total remuneration (inclusive of base salary and superannuation, and, where applicable, performance payments).

Legal change

New legislation

Responding to the Australian Universities Accord Final Report

The Australian Government made changes to the Higher Education Support Act 2003 and other related legislation to respond to the recommendations of the final report of the Australian Universities Accord Review. The changes:

- require higher education providers to ensure that 40 per cent of the Student Services and Amenities Fees (SSAF) revenue they collect from students is provided to student-led organisations
- affect the way HELP indexation is calculated to use the lower of either the consumer price index or the wage price index backdated to the 2023 and 2024 indexation years
- establish a Commonwealth Prac Payment from 1 July 2025 for student teachers, nurses, midwives and social workers
- provide greater opportunities for more people, especially those from underrepresented backgrounds, to participate in higher education by delivering FEE-FREE Uni Ready courses.

The Australian Government also amended the Ombudsman Act 1976 to establish the National Student Ombudsman as a new statutory function of the Commonwealth Ombudsman to deal with complaints about, and conduct investigations into, actions of higher education providers. The new Ombudsman is able to take complaints from 1 February 2025.

Changes to process offshore student visa applications

On 18 December 2024, the Assistant Minister for Citizenship and Multicultural Affairs made Ministerial Direction 111 (Order for considering and disposing of offshore Subclass 500 (Student) visa applications). The ministerial order introduces new arrangements for processing offshore subclass 500 (student) visa applications. It provides an order of priorities for considering and disposing of applications, whereby each higher education and VET provider is allocated a priority threshold. The priority threshold is set at 80% of the indicative allocation of new overseas student commencements as calculated by the Department of Education in late 2024. Applications are processed as high priority as long the providers remain below their priority threshold, and move to standard priority once the threshold is exceeded.

Changes to Australia's national security laws

The Australian Government implemented significant changes to export controls laws through amendments to the Defence Trade Controls Act 2012. The amendments implement Australia's commitments under the AUKUS agreement, including removing the need to obtain a permit for supply of most controlled items between Australia, the United Kingdom and the United States. The amendments also introduce 3 new serious criminal offences for engaging in certain conduct related to items on the Defence and Strategic Goods List (DSGL) without a permit, unless an exception applies.

UTS has audited existing research projects to ensure compliance and modified the research project risk assessment process to identify any new projects that may require permits.

The Australian Government also amended the Defence Act 1903 to create the Safeguarding Australia's Military Secrets program. The changes establish a framework to regulate the work that certain former defence staff members (foreign work restricted individuals) can perform without a foreign work authorisation; and the training that Australian citizens and permanent residents, other than foreign restricted individuals, may provide without a foreign work authorisation. The requirement for a foreign work authorisation strengthens Australia's security by preventing individuals from disclosing or exploiting classified military or related information. General and targeted information has been circulated to staff as to how to comply with this new legislation.

The government also amended the Australian Research Council Act 2001 to grant the minister the power to terminate a funding approval of an organisation for reasons of the security, defence or international relations of Australia. The minister will also have the power to direct the board not to approve a grant, or to terminate funding to research grants, based on national security concerns.

New foreign bribery offence

The Australian Government has strengthened the legal framework by introducing a new strict liability offence for failing to prevent foreign bribery through amendments to the Criminal Code Act 1995. As a defence, body corporates, including universities, will need to prove they adopted adequate procedures to prevent the bribery. UTS has amended relevant policies and procedures to respond to the new offence.

Fair Work Legislation Amendment (Closing Loopholes) Acts

The Australian Government's 'Closing Loopholes' workplace reforms are being enacted through amendments to the Fair Work Act 2009 and related legislation. Key changes which came into effect in 2024 affecting the higher education sector include:

- a new 'right to disconnect' for employees to refuse to read, respond or monitor communication from employers or third parties outside their paid working hours unless that refusal is unreasonable
- changes to the definition of 'casual employee' mean that a broader range of matters must be taken into consideration when determining whether an employee is a casual employee or not
- a new 'employee choice pathway' for eligible employees to change to full-time or part-time (permanent) employment if they want to.

New industrial manslaughter laws

The NSW Government introduced a new industrial manslaughter offence under the Work Health and Safety Act 2011. Significant penalties now apply for conduct that causes the death of a worker, with fines of up to $20 million for companies and up to 25 years' imprisonment for individuals.

Significant cases

Significant cases affecting the higher education sector in 2024 include the following.

TEQSA v Chegg Inc

Enforces academic integrity laws and sets a precedent for regulatory action against academic cheating services, thereby protecting the quality and reputation of higher education in Australia.

Hove v University of Western Australia [2024] WASCA 37

Affirms the importance of education providers ensuring that they follow their internal procedures and provide procedural fairness when deciding whether to exclude students from enrolling in practical clinical units.

Fair Work Ombudsman v University of Melbourne [2024] FCA 330

Illustrates the importance of protecting casual academic employees' workplace rights. Universities must ensure that employees can make complaints or inquiries about their employment without fear of adverse action. The penalties imposed by the FWO will serve as a deterrent to other institutions, emphasising the need for compliance with workplace laws and the fair treatment of casual employees at universities.

University of Sydney v National Tertiary Education Industry Union [2024] FCAFC 57

Highlights the need for clear guidelines and standards for academic conduct, particularly in relation to public commentary, and emphasises the importance of ensuring that disciplinary actions are based on well-defined and consistently applied standards to avoid potential legal challenges.

GGG v University of Sydney [2024] NSWCATAD 264

Underscores the need for universities to ensure that their actions, particularly those involving the collection and use of employee information, comply with relevant privacy laws and emphasises the significance of clear and transparent communication between universities and their employees regarding external interests and potential conflicts of interest.

Cybersecurity

UTS recognises that having strong cybersecurity capabilities enables the organisation to achieve its priorities in a safer manner. UTS maintained its focus on enhancing its cybersecurity posture and maturity during 2024, building on the robust foundations established during previous years.

The Chief Information Security Officer reported to the Audit and Risk Committee every meeting (5 during the year), and management also presented a report to the UTS Council. These reports cover progress made in delivering the comprehensive cybersecurity roadmap and call out any changes in the cyber risk environment driven by either internal or external influences.

UTS experienced no significant cybersecurity incidents in 2024. Due to improved detection and monitoring capabilities the cyber team were able to detect a few concerning behaviours early and responded effectively to reduce the risk exposure. Examples include UTS websites that may lack protective features or older non-secure devices running on the UTS network that required removal or remediation activity.

The critical area of 'cyber aware people' saw a new emphasis in 2024 with the creation of a new manager role focused on cybersecurity engagement and awareness. This increased the capacity for relevant outreach activities across UTS involving faculties, business units, events and tailored sessions, and a refresh of the cybersecurity champions network, which has been running for 18 months.

Selected 2024 milestones include:

- as part of the wider Information Technology Unit (ITU) operating model changes, the cybersecurity team redefined its roles and converted a few critical positions to continuing roles. This provides increased stability and continuity in building resilience within the team
- conducted multiple engagement sessions with faculty and business unit leadership teams and town halls to spread cyber safe behaviours and tailor activities to local requirements
- delivered a significant uplift in security for access of guest users into the UTS Teams environment by reviewing and deleting unused access and introducing multifactor authentication to all guest users
- strengthened the security around multifactor authentication for all UTS staff by shifting away from the SMS option to using a more robust method (this process has also commenced for all UTS students)
- greatly improved email security across UTS through the implementation of domain-based message authentication, reporting and conformance (DMARC), which is an increasingly mandatory requirement for email to flow smoothly between organisations
- published 2 new information security directives to include necessary updates and changes
- delivered the secure reference architecture framework and associated security designs, which are a substantial step towards embedding security by design within IT solutions and services
- undertook improvement work with the managed Security Operations Centre to increase detections tailored to a university environment and effective triage and alerting, and
- implemented the Centre for Internet Security benchmark controls for ITU assets to improve cybersecurity controls to protect against cyber threats.

Land disposals

UTS sold Blackfriars land and building in September 2024 for $53,164,000. The funds from the sale were subsequently invested in UTS managed funds, Australian Ethical Limited.

Overseas travel and promotion

UTS paid $8,508,000 for overseas travel in 2024 (compared with $8,965,000 in 2023). These payments supported a wide range of activities, including attendance and presentation of research papers at international conferences, staff development, research and teaching at affiliated institutions.

Privacy

UTS is bound by the 12 information protection principles contained within the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act). This Act covers the university in relation to how it manages personal information on or after 1 July 2000, and health information on or after 1 July 2000 until 1 September 2004.

UTS is also bound by the 15 health privacy principles contained within the Health Records and Information Privacy Act 2002 (NSW) (HRIP Act). This Act covers the university in relation to how it manages health information on or after 1 September 2004.

Although UTS is not directly covered by the Privacy Act 1988 (Cwlth), its principles may apply in certain circumstances in relation to university activities that are governed by other federal legislation or codes of practice, as well as data breach reporting in relation to certain types of information. Similarly, in some cases, provisions of the European Union's General Data Protection Regulation (GDPR), China's Personal Information Protection Law (PIPL), or other cross-jurisdictional privacy laws in other countries, may apply to data in some limited activities.

How UTS manages personal and health information

The management of personal and health information is primarily governed by the university's Privacy Policy and the Privacy Management Plan. The Privacy Management Plan is required under the PPIP Act and is essentially a statement of how UTS complies with both New South Wales privacy acts.

The plan includes information about:

- UTS policies and practices that govern privacy
- details of information and training programs for staff
- how UTS will comply with information protection and health privacy principles including details of how UTS collects, uses and protects information, and examples of when information may be disclosed
- details of the university's internal review process, and
- a summary of the types of information UTS collects and holds.

Both the policy and the plan are available on the university's public website. Privacy is also supported by the Data Breach Policy, Data Governance Policy, Records Management Policy, Artificial Intelligence Operations Policy and other activity-based policies which may include privacy requirements where appropriate.

More specific information may also be provided through privacy notices (collection statements) provided at the time an individual's information is being collected. These notices will explain what is being collected, how that information will be used, if it is expected to be disclosed and an individual's rights. Key privacy notices are located on the university's website footer.

Activities during 2024

- We continue to focus on building privacy into information system design and development as part of the project planning stage. Privacy is considered of high importance by project teams where a new system may involve personal or health information.
- Our Privacy Contact Network continued with 2 sessions held for our privacy champions across the university.
- Further work has been undertaken to streamline and refine our privacy content and transparency communications, in particular in consolidating key privacy notices. Our student focused notices were reviewed in 2024 along with the privacy content in our Student Declaration. As a result, relevant privacy content was consolidated into a newly deployed Student Privacy Notice that covers both applicants and students. This work aimed to improve transparency and reduce duplication, making it easier for students to understand how their information will be handled. Further work in streamlining privacy notices and content will continue into 2025.
- We continue to improve data retention by reviewing records and data collections to ensure they can be destroyed when they are no longer required to be retained, and ensuring they are stored in appropriate systems while ongoing retention is required.
- The new Mandatory Notification of Data Breach (MNDB) Scheme under the PPIP Act, introduced in late 2023, was applied to incidents identified in 2024. Potential data issues were considered in line with the Data Breach Policy, and notification obligations were assessed and applied where required.
- An annual review of the Data Breach Policy was conducted with minor amendments applied in November.

Internal reviews

We completed 2 formal privacy internal reviews during 2024 under section 53 of the PPIP Act. These reviews were conducted within the required timelines and framework of the university's obligations under the PPIP Act.

Right to information

Review of proactive release program

Under section 7 of the Government Information (Public Access) Act 2009 (NSW) (GIPA Act), agencies must review their programs for the release of government information to identify the kinds of information that can be made publicly available. UTS's program for the proactive release of information involves decisions made at the business activity level routinely regarding what information to make public on the university's website. Consideration of proactive release is undertaken on an ongoing basis, and considered annually by the right to information team.

Information relating to ongoing business and key projects and activities considered of interest to the wider community is proactively released on the UTS website.

- News: The UTS Newsroom includes news stories of interest, including media releases, and informs the public of activities happening at UTS.
- Sustainability: UTS strives to continually improve its sustainability performance. Information is available on the UTS website relating to our targets, sustainability-related activities and performance.
- Facts, figures and ratings: Information known to be of interest to the public includes information on the university's ratings against other universities, and facts and figures including information on student numbers, diversity, performance and completion rates, and graduate employment. This information is released for the benefit of past, present and future students, as well as donors, partners and supporters.
- Governance: The GIPA Act requires certain governance information to be made public, such as policy documents. These are available on the UTS website. Additional governance information is proactively released to inform staff, students and members of the public about the governance frameworks at UTS and important university decisions. Governance information proactively released includes information about the UTS Council and Academic Board and associated committees.
- Partnerships: In response to information requests during 2024, information about defence-related partnerships was proactively released and is available on our website.

In addition to the above, the review focused on trends identified through requests for information, including applications under the GIPA Act. Any information available regarding informal requests was also considered. No trends in requests were identified. As a result no further information was proactively released.

Number of access applications received

In 2024, UTS received a total of 14 access applications, of which 7 became valid access applications.

No applications processed in 2024 were carried over from 2023, and no access applications received in 2024 were still being processed into 2025.

Number of refused applications for Schedule 1 information

During the reporting period, no applications were refused due to a conclusive public interest against disclosure under Schedule 1 to the GIPA Act.

Statistical information about access applications

Table A: Number of applications by type of applicant and outcome[1]

	Access granted in full	Access granted in part	Access refused in full	Information not held	Information already available	Refuse to deal with application	Refuse to confirm/deny whether information is held
Media	0	0	0	0	0	0	0
Members of parliament	0	0	0	0	0	0	0
Private sector business	0	0	0	0	0	0	0
Not–for–profit organisations or community groups	1	1	0	1	0	0	0
Members of the public (application by legal representative)	0	0	0	0	0	0	0
Members of the public (other)	2	3	1	3	2	1	0

1. More than one decision may be made in respect of a particular access application. Where this is the case, each decision is individually recorded.

Table B: Number of applications by type of application and outcome[1]

	Access granted in full	Access granted in part	Access refused in full	Information not held	Information already available	Refuse to deal with application	Refuse to confirm/deny whether information is held
Personal information applications[2]	0	0	0	0	0	0	0
Access applications (other than personal information applications)	3	4	1	4	2	0	0
Access applications that are partly personal information applications and partly other	0	0	0	0	0	1	0

1. More than one decision can be made in respect of a particular access application. Where this is the case, each decision is individually recorded.
2. A personal information application is an access application for personal information (as defined in clause 4 of Schedule 4 to the GIPA Act) about the applicant (the applicant being an individual).

Table C: Invalid applications

Reason for invalidity	Number
Application does not comply with formal requirements (s 41)	9
Application is for excluded information of the agency (s 43)	0
Application contravenes restraint order (s 110)	0
Total number of invalid applications received	**9**
Invalid applications that subsequently became valid applications	2

Table D: Conclusive presumption of overriding public interest against disclosure: matters listed in Schedule 1 to the GIPA Act[1]

Overriding public interest against disclosure	Number of times consideration used
Overriding secrecy laws	0
Cabinet information	0
Executive Council information	0
Contempt	0
Legal professional privilege	0
Excluded information	0
Documents affecting law enforcement and public safety	0
Transport safety	0
Adoption	0
Care and protection of children	0
Ministerial code of conduct	0
Aboriginal and environmental heritage	0
Information about complaints to Judicial Commission	0
Information about authorised transactions under Electricity Network Assets (Authorised Transactions) Act 2015	0
Information about authorised transaction under Land and Property Information NSW (Authorised Transaction) Act 2016	0

1. More than one public interest consideration may apply in relation to a particular access application and, if so, each such consideration is to be recorded (but only once per application).

Table E: Other public interest considerations against disclosure: matters listed in table to section 14 of the GIPA Act[1]

Public interest considerations against disclosure	Number of occasions when application not successful[1]
Responsible and effective government	2
Law enforcement and security	0
Individual rights, judicial processes and natural justice	3
Business interests of agencies and other persons	4
Environment, culture, economy and general matters	1
Secrecy provisions	1
Exempt documents under interstate freedom of information legislation	0

1. More than one public interest consideration may apply in relation to a particular access application and, if so, each such consideration is to be recorded (but only once per application).

Table F: Timeliness

Timeliness	Number of applications
Decided within the statutory timeframe (20 days plus any extensions)	6
Decided after 35 days (by agreement with applicant)	0
Not decided within time (deemed refusal)	1[1]
Total	**7**

1. One access application was completed 5 working days after the due date. Attempts were made to negotiate an extension with the applicant but no response was received from them until after the application was decided.

Table G: Number of applications reviewed under Part 5 of the GIPA Act (by type of review and outcome)

Type of review	Decision varied	Decision upheld	Total
Internal review	0	1	1
Review by Information Commissioner	0	0	0[1]
Internal review following recommendation under section 93 of the GIPA Act	0	0	0
Review by NSW Civil and Administrative Tribunal	0	0	0
Total	**0**	**0**	**1**

1. One application has been referred to review by the Information Commissioner in late 2024. The review was not completed in 2024. It will be reflected in the 2025 annual report.

Table H: Applications for review under Part 5 of the GIPA Act (by type of applicant)

Type of applicant	Number of applications for review
Applications by access applicants	2
Applications by persons to whom information the subject of access application relates (s 54)	0

Table I: Applications transferred to other agencies under Division 2 of Part 4 of the GIPA Act (by type of transfer)

Type of transfer	Number of applications transferred
Agency–initiated transfers	0
Applicant–initiated transfers	0