Fraud and Corruption Control Policy

Section 1 - Overview and Scope

(1) The purpose of this Policy is to protect the reputation and assets of the University of New England (UNE) from fraudulent and corrupt activities, and outline the processes and mechanisms for preventing, reporting and investigating incidents of fraudulent activity in and against the University.

(2) This Policy establishes a Fraud and Corruption Control System (FCCS) consistent with the Australian Standard on Fraud and Corruption Control (AS 8001:2021). The Policy provides guidance on how to prevent, detect and respond to incidents of fraud and corruption and:

a. reinforces management's commitment to, and responsibility for, identifying risk exposures to fraudulent and corrupt activities, and ensuring all UNE Representatives and students are aware that UNE has zero tolerance for fraud or corrupt conduct; and
b. requires UNE Representatives to perform their duties with honesty and integrity in accordance with the framework of ethical conduct that underpins the expected standards of behaviour for all members of the University community. The Code of Conduct policy sets the standards of ethical behaviour expected of staff and students. Staff should abide by the principles set out in the Code of Conduct and students should abide by principles set out in the Student Behavioural Misconduct Rules.

(3) This Policy applies to all UNE Representatives, students, customers, contractors, business associates, partners, external service providers, volunteers and controlled entities of UNE. Fraud and corruption prevention, control and reporting is the responsibility of all UNE Representatives.

a. Staff and other individuals who enter into a range of relationships with the University (including contractors, visiting fellows and volunteers) have a responsibility to act honestly, responsibly and impartially in accordance with the Code of Conduct.

(4) This Policy should be read in conjunction with the UNE Risk Management Policy, Organisational Resilience Rule, Procurement Policy, and Codes of Conduct.

(5) Within this Policy:

a. Part A sets out the Principles that underpin this Policy;
b. Part B outlines UNE's approach to planning and preventing fraud and corruption;
c. Part C outlines UNE's systems for detecting fraud and corruption; and
d. Part D outlines UNE's responses to fraud and corruption.

Section 2 - Policy

Part A - Principles

(6) UNE has zero tolerance for fraudulent or corrupt activity.

(7) UNE recognises that fraud and corruption create reputational and financial damage to the University.

(8) UNE recognises that the risk of fraud and corruption can arise in various contexts and has put in place measures proportionate to the risks in order that UNE Representatives, students and associates of the University and its controlled entities are aware and understand the relevant policies for the prevention, detection and response to fraud and corruption.

(9) To demonstrate this commitment the University, through the Vice-Chancellor and Chief Executive Officer (VC&CEO) and Senior Executive, will ensure:

a. the integration of fraud and corruption risk management into the University's values, practices and business plans;
b. that the risk of fraud and corruption is assessed and that risk assessment will be conducted:
    i. following substantive changes to the regulatory or compliance environment;
    ii. following substantive changes to the mechanisms in place at the University to manage fraud and corruption risk;
    iii. following detection of substantive fraud or corruption; and/ or
    iv. at least every two years.
c. the effectiveness of mechanisms to control fraud and corruption risk are evaluated;
d. the investigation of suspected fraud or corruption and take appropriate disciplinary action, which may include referral to the relevant police service, for any person found to have engaged in fraud or corruption;
e. the reporting of suspected corruption, whether it involves a UNE Representative or not, to the relevant anti-corruption agency where required by law;
f. in the absence of criminal prosecution, the application of appropriate civil, administrative or disciplinary penalties against individuals who have been party to fraud or corruption;
g. the taking of reasonable legal action to recover losses that result from fraudulent or corrupt conduct;
h. cooperation with the agencies including ICAC, the NSW Ombudsman, Audit Office of NSW and NSW Police Force (or the equivalent agency/ies in another state or territory as applicable) in relation to fraud and corruption and wherever practical, the alignment of University processes to better practice advice issues by those organisations;
i. the recording of all suspected incidents of fraud and corruption to identify trends and prevent recurrence;
j. the reporting of all actual and suspected fraud and corruption to the VC&CEO and the Audit and Risk Committee; and
k. the due consideration of a fidelity guarantee policy to protect the University against the financial consequences of fraud.

Framework of ethical conduct

(10) This Policy is one element of a suite of practices in place across the University that reinforce the University's values. The University's framework of ethical conduct includes, but is not limited to:

a. UNE Governance, Integrity and Standards Policy, Code of Conduct, Conflicts of Interest Policy and other University Policies specifically intended to guide positive behaviour;
b. the mandate and commitment to fraud and corruption control made in this Policy;
c. example setting by senior management;
d. roles and responsibilities as articulated in University Policies, including the position descriptions, and the UNE Delegations Framework Rule;
e. mechanisms for reporting and managing wrongdoing and misconduct;

f. complaints management processes; and
g. mechanisms to ensure ethical standards in research and academic integrity.

(11) Supporting the University's commitment to an observable ethical culture, all staff are required to confirm in writing, annually that they have over the previous twelve months complied with the University's Code of Conduct and this Fraud and Corruption Control Policy, and that they will continue to comply over the ensuing twelve months.

Part B - Planning and prevention of fraud and corruption

Fraud control officer

(12) The Director Governance and University Secretary (DGUS) is the primary Fraud and Corruption Control Officer (FCCO). In relation to fraud and corruption, the DGUS is responsible for:

a. developing, implementing and maintaining the University's FCCS; and
b. coordinating periodic assessment of the University's fraud and corruption risks.

(13) The Head, Internal Audit is responsible for:

a. recording fraud and corruption events;
b. escalating and monitoring fraud and corruption events including coordinating internal and external reporting; and
c. conducting, coordinating or monitoring investigations into allegations of fraud and corruption.

(14) While not limiting the capacity of any person to report matters of concern to any person or agency, the Head, Internal Audit is the nominated position to make official report to external agencies as a representative of the University with the exception of:

a. the VC&CEO, as the principal officer of the University, has a non-delegable duty to report to the ICAC as soon as they become aware of any matter that they suspect concerns and may concern corrupt conduct.

(15) The Senior Executive is responsible for ensuring that all of the University's fraud and corruption control resources are coordinated and work together to fulfil the objectives of this Policy and the Fraud and Corruption Control System (FCCS).

(16) The Chief Information Security Officer (CISO) is responsible for:

a. establishing and monitoring systems-based controls and reporting on matters of concern to the Head, Internal Audit on the University's fraud and corruption exposures;
b. attending continuing professional development in technology-enabled fraud and corruption in order to maintain a sound understanding of methods for managing the risk of fraud and corruption in accordance with relevant standards and contemporary and emerging practice in the field;
c. maintaining a sound understanding of how an information security management system can effectively mitigate the risks of fraud and corruption; and
d. maintaining a sound understanding of cybercrime and methods for managing the risk of cybercrime in accordance with relevant standards and contemporary and emerging practice in the field.

Prevention systems

(17) UNE is committed to preventing fraud and corruption within the University and its controlled entities. The enact this commitment, UNE will put in place appropriate mechanisms for fraud and corruption risk management, including

policies and processes, risk assessment, internal controls, investigation, reporting, education and independent auditing to reduce the incidence of fraud and corruption and regularly evaluating these.

(18) UNE will minimise the incidence of fraud and corruption by:

a. applying the Risk Management Policy and Risk Management Policy - Annexure 1 - Risk Approach and Terminology;
b. making all UNE employees, and employees of controlled entities, aware of UNE's Code of Conduct, Conflicts of Interest Policy and other elements of the UNE ethical conduct framework at induction and throughout employment;
c. the establishment and implementation of processes for all students to be made aware of the University's Code of Conduct, Student Behavioural Misconduct Rules, and other relevant Codes and Policies;
d. the establishment and implementation of management accountabilities, including:
    i. the incorporation of fraud and corruption control into the performance management system; and
    ii. allocating, as far as practicable any losses, either known or estimated, due to fraud and corruption to the cost centre in which the loss occurred;
e. the establishment and implementation of first line assurance business practices for preventing fraud and corruption that are:
    i. developed in all relevant areas of the University where there is a risk of fraudulent or corrupt activities;
    ii. identified as required by assessment of the risk of fraud or corruption;
    iii. documented and include requirements to create records of performance of the process;
    iv. approved by a manager with sufficient skill, competence and accountability to validate the business process will be effective in the prevention of fraud and corruption; and
    v. periodically subject to informal and formal audit.
f. the inclusion of fraud and corruption control responsibilities for manager and all members of staff in the Delegations Register;
g. the establishment and implementation of a program for the communication of awareness in relation to the risk of fraud and corruption; and
h. the establishment and implementation of processes for:
    i. employment screening and relevant employee declarations;
    ii. the vetting of business associates (suppliers);
    iii. the vetting of education agents, intermediaries and partners;
    iv. vetting of student academic capability;
    v. the protection of academic and research integrity;
    vi. the protection of intellectual property;
    vii. the protection of the integrity of certification documentation; and
    viii. the protection of any personal information collected by the University.

Fraud and corruption risk management

(19) The DGUS will coordinate an annual program of fraud and risk assessment management activities across the University. The program:

a. will be submitted to the Audit and Risk Committee for endorsement;
b. will be developed using a risk-based approach to address the areas of greatest risk exposure first as determined through application of risk assessment methodologies identified in the Risk Management Policy and Risk Management Policy - Annexure 1 - Risk Approach and Terminology;

c. will be continuously improved having regards to:
    i. risk reviews undertaken;
    ii. the records of risk exposure in the Enterprise Risk Management Register;
    iii. the historical incidence of fraudulent or corrupt incidents;
    iv. the guidance material incorporated in AS80001:2021; and
    v. external environment scanning including global, national and higher education sectors.

(20) The Head, Internal Audit will use the findings of the fraud and corruption risk assessments to develop a fraud and corruption control assurance management plan to be reported annually to the Audit and Risk Committee and monitored for effectiveness over time.

Communication and awareness of fraud and corruption

(21) The DGUS will coordinate a regular program of communication and awareness to inform all stakeholders impacted by this Policy of:

a. UNE's definition of behaviours that constitute fraud or corruption;
b. UNE's zero tolerance position for fraud and corruption;
c. the general incidence of fraud and corruption;
d. fraud and corruption exposures in the higher education sector;
e. the assessed fraud and corruption exposures within UNE;
f. the types of fraud and corruption that have been identified at UNE in the past five years and how these were dealt with in terms of disciplinary action and internal control enhancements;
g. the expectations of management and staff if fraud or corruption is detected or suspected;
h. fraud and corruption processes for management and staff including the Reporting Wrongdoing at UNE Policy and overview of the University's FCCS;
i. an overview of fraud and corruption red flag behaviours.

Employment screening and vetting processes

(22) The Director People and Culture, will develop, implement and coordinate an employment screening program consistent with contemporary human resource practice, relevant legislation, codes and standards. The employment screening program will apply to appointments of:

a. senior executives and senior management; and
b. positions where the University faces an exposure to fraud and corruption above that of the level from professional and academic staff.

(23) The program will provide for effective employment screening of relevant persons:

a. before appointment;
b. on promotion or change of employment circumstances;
c. on temporary transfer/ secondment to an acting role of more than six months duration; and
d. at recurring intervals of not more than three years.

(24) The Director People and Culture will develop, implement and coordinate business processes for the declaration of:

a. outside professional activities; and
b. declarations of conflicts of interest.

Business associate (supplier) vetting

(25) The Chief Financial Officer (CFO) will develop, implement and coordinate a process for the vetting of business associates (suppliers). The vetting process:

a. must be applied to all business associates with whom the University has an annual spend threshold of $150,000 or more;
b. may be applied to other business associates, subject to resource availability to undertake the vetting;
c. is to be repeated every two years for all business associates.

(26) The vetting process is to include but is not limited to the following:

a. search of company register;
b. ABN and bank account confirmation;
c. verification of the personal details of directors;
d. director bankruptcy search;
e. disqualified director search;
f. educational qualifications claimed;
g. assessment of credit rating;
h. search of legal proceeding pending and judgements entered;
i. telephone listing and trading address;
j. media search;
k. search of available debarment, sanction and watch-lists; and
l. Search for politically exposed persons.

(27) Vetting is to be undertaken prior to the award of contracts exceeding the threshold value and at such time that the University becomes aware that expenditure with a specific supplier has exceeded the annual threshold value.

(28) Adverse outcomes in relation to vetting are to be report to the Chief Operating Officer (COO) for consideration of the University's ongoing commercial relationship with the business associate.

Physical security and asset management

(29) The COO will maintain oversight of the University's practices for the physical security and asset management. The security of the physical environment will be assessed to ensure appropriate measures are implemented for the prevention of theft of valuable tangible assets. Details of measures in place are outlined in the Key and Lock Policy, Password Policy, IT Server Room Access Procedures, and Information and Communications Infrastructure Rule.

Education agent, intermediary and partner vetting

(30) For Education agent, intermediary and partner vetting process refer to the Academic Quality Assurance Policy and Third Party Provider Arrangements Policy.

Student capability vetting

(31) For student capability vetting see the Admission, Credit and Enrolment Policy.

a. Where UNE accepts student admitted through other providers and third parties, the Executive Principal Brand Partnerships and Business Development will ensure vetting of students is at least equivalent to the standards undertaken by UNE.

(32) Verification of student identity occurs at the point of issuing a student identification card.

Protection of academic and research integrity

(33) The Student Coursework Academic Misconduct Rule and Student Academic Integrity Policy, HDR - Higher Degree Research Student Responsible Research Conduct Policy and the Code of Conduct for Research Rule set out the requirements for the protection of academic and research integrity.

Protection of intellectual property

(34) The Knowledge Assets and Intellectual Property Policy sets out the requirements for the protection of intellectual property.

Protection of certification documentation

(35) The University Seal and Signing Documents Rule, Academic Qualifications Issuance Policy, Rescission of an Award/Correction of an Award Procedure and Digital Signatures Policy outline business practices protecting the integrity of the certification of documents.

(36) Business practices must ensure all certification documentation issued by the University is:

a. unambiguously issued by UNE;
b. readily distinguishable from other certification documents issued by UNE;
c. protected against fraudulent use, including implementing practices to:
    i. secure and account for paper stocks used in the production of certification documentation, and
    ii. ensure the storage of electronic records of certification documentation in accordance with the Records Management Rule and Records Management Procedures.
d. traceable and authenticable;
e. designed to prevent unauthorised reproduction; and
f. replaceable only through an authorised and verifiable process.

Privacy management

(37) The DGUS will promote the development, implementation and coordination of business practices to protect the integrity of personal information.

(38) These practices must ensure all personal information is compliant with relevant statutory and regulatory requirements and the information protection principles applying the NSW public sector agencies. The UNE Privacy Management Rule outlines the business practices to protect the personal information UNE collects.

Internal audit

(39) Internal Audit support the prevention of fraud and corruption by:

a. evaluating the effectiveness of internal controls in mitigating the risk of fraud and corruption;
b. developing a risk-based internal audit program that considers the risk of fraud and corruption in line with the UNE Internal Audit Charter; and
c. periodically reviewing the effectiveness of the University's fraud and corruption prevention framework including this Policy and the FCCS.

Part C - Detecting fraud and corruption

(40) UNE is committed to the development and implementation of dynamic detection processes. The DGUS, CISO, Head of Finance and Head, Internal Audit have responsibility to validate the development of systems to detect and investigate fraud and corruption, including post transactional review, data mining and analysis of management accounting reports.

Post-transactional reviews

(41) A random selection of transaction will be reviewed after processing, by staff unconnected with the business unit making the transaction. Transaction to be reviewed include any action where fraudulent or corrupt gain or loss is possible and includes:

a. financial transactions;
b. student admission transaction;
c. transactions related to the production of certification documentation;
d. staff administration transactions;
e. recruitment and selection transactions;
f. tender selection and procurement transactions; and/ or
g. any other are of transaction that the Head, Internal Audit deems reasonable or necessary.

(42) The transaction reviews will look to ensure:

a. relevant documentation relating to the transaction is available and complete; and
b. transaction authorisations are properly made and recorded.

Data analytics

(43) Data analytics will be developed to consider relevant indicators of the University's fraud and corruption risk exposure. Data analysis will be used to identify suspect transitions.

Analysis of accounting reports

(44) Analysis of accounting reports will be conducted to identify trends that may be indicative of fraud or corrupt conduct, including:

a. monthly actual/ budget comparison reports at account code level;
b. reporting comparing expenditure against industry benchmarks;
c. reports highlighting unusual trends on bad or doubtful debts.

Student related fraud and corruption detection systems

(45) Refer to relevant policies including Admission, Credit and Enrolment Policy, Student Behavioural Misconduct Rules, Student Coursework Academic Misconduct Rule and Student Academic Integrity Policy, HDR - Higher Degree Research Student Responsible Research Conduct Policy, Assessment Policy, and HDR - Encumbrances Procedure.

External audit

(46) UNE will present the annual financial statements to the NSW Audit Office for validation, and will participate in audits by the NSW Audit Office, and any other statutory agency as required.

Part D - Response to fraud and corruption

Reporting fraud and corruption

(47) UNE Representatives have a duty to report fraud and corruption, and the University encourages reporting of reasonable suspicions in relation to the University.

(48) UNE may have a statutory, regulatory or contractual obligation to report suspected fraud and/ or corruption to an external body or agency.

(49) UNE does not tolerate vexatious and/ or frivolous reports in relation to fraud or corruption, and may initiate disciplinary proceedings where reports of this nature are made.

(50) Reporting may be done by following the process outlined in the Reporting Wrongdoing at UNE Policy.

Complaint management

(51) UNE's complaint management processes are designed to ensure that staff receiving complaints are trained to recognise complaints about fraud and corruption and the internal and external reporting processes that are available.

Exit interviews

(52) UNE's exit interviews seeks to identify knowledge or reasonable suspicion the exiting employee has of potential fraudulent or corrupt conduct, including the conduct of the exiting employee, other internal UNE persons, and business associates of internal UNE persons.

Investigation of fraud and corruption

(53) The investigation of a report of possible wrongdoing to an authorised disclosure officer will be managed as outlined in the Reporting Wrongdoing at UNE Policy.

Responses to privacy concerns

(54) Concerns related to personal information held by the University will be address in accordance with the Privacy Management Rule.

Responsibilities

(55) The following table outlines responsibilities associated with this procedure:

Officer or body	Responsibilities
Council	Approve the University's Fraud and Corruption Control Policy and System; Receive reports of significant instances of fraud and remedial actions taken.
Audit and Risk Committee	Review and advise Council on the appropriateness of the University's process for effective identification and management of fraud and corruption risks; Endorse the University's Fraud and Corruption Control Policy and System; Receive reports on instances of 'high' and 'extreme' risks reported by Business units of the University and review the remedial actions taken.
Vice-Chancellor and Chief Executive Officer (VC&CEO)	Foster an environment that makes active fraud and corruption control the responsibility of all staff. Ensure that appropriate measures are in place in relation to fraud prevention and detection; Report any matter they suspect may concern corrupt conduct to the ICAC (non-delegable duty) Ensure appropriate resourcing within Governance Division to lead fraud control at the University.

Officer or body	Responsibilities
University Executive	Foster an environment that makes active fraud and corruption control the responsibility of all staff; Ensure that appropriate measures are in place with regard to fraud and corruption prevention and detection.
Chief Operating Officer	With advice from the Legal Office, refer instances of potential serious or complex fraud offences to the NSW Police or external agency as appropriate.
Director Governance and University Secretary (DGUS)	Arrange fraud and corruption awareness training for relevant staff. Coordinate fraud and corruption risk assessment activity across the University;
Head, Internal Audit	Develop the University's Fraud and Corruption Control Policy and System; Use fraud risk assessments to inform the development of the University's annual internal audit program for endorsement by the ARC and approval by Council; Receive reports of suspected fraud and take appropriate action.
Chief Financial Officer (CFO)	Review, on an ongoing basis, the financial fraud controls to ensure they are effective in minimising financial fraud risks; Provide assurance on the adequacy of the University's financial fraud control arrangements to the external auditors annually, through management representation letters.
Heads of Business units	Foster an environment that makes fraud and corruption control the responsibility of all staff; Ensure that a fraud and corruption risk assessment for their area is conducted and reviewed at least every two years and whenever there is significant organisational change; Ensure that appropriate internal controls are in place and operating effectively to minimise fraud and corruption risks (including by ensuring appropriate record keeping practices are in place); Ensure that staff participate in fraud and corruption awareness education and training; Ensure that agreed recommendations relating to fraud and corruption in internal and external audit reports are implemented promptly.
All UNE Representatives and students	Act in accordance with the Code of Conduct policy and Student Behavioural Misconduct Rules when undertaking their duties and representing the University; Disclose to their supervisor any conflict of interest that relates to the affairs of the University; Actively participate in the implementation of fraud risk control strategies; Undertake appropriate record keeping; Report any suspicions of, or information relating to any instance of, fraudulent or corrupt conduct to their supervisor, an authorised officer for Reporting Wrongdoing at UNE Policy or the DGUS; Encourage others to make such reports; Deal with all reports of suspected fraud or corruption professionally and promptly.

(56) The following Table provides examples of functions and activities that are at risk of fraud and corruption, noting these are not exhaustive.

AREA OR FUNCTION	EXAMPLES
Misuse of University assets and monies	Use of UNE funds or resources for personal use, and not reimbursed to the University; Unauthorised sale of UNE assets for personal gain, or sale at values that are not arms length; Theft of UNE property such as cash and/ or equipment; Dishonestly using the University's computers, vehicles, telephones, credit cards, cab vouchers, stationery, other property and/ or services; Dishonestly using grant of research funds or scholarships for other than purposes for which they were provided.
Travel	Claiming for a travel entitlement to attend a course and then not attending the course and not reimbursing travel monies; Luxurious or excessive expenditure; Inflated and/ or fake claims; Undertaking travel under the guide of a business purpose when the dominant purpose and expenditure of time was for a private holiday/ or other private purpose.

AREA OR FUNCTION	EXAMPLES
IT Assets and Security	Misappropriation or the unauthorised or unlawful destruction of data; Unauthorised or unlawful alteration of data; Accepting bribes for admission of students or creating fraudulent transcripts for students.
Regulatory Compliance	Providing false or misleading information to agencies such as the NSW Ombudsman, the NSW Audit Office or TEQSA; Failing to provide information where there is a legal obligation to do so.
Contract Management	Receiving kickbacks or secret commissions from a contractor; Accepting hospitality from suppliers which is either not approved in accordance with the UNE Gifts and Benefits Policy, or is deemed to be excessive and not incidental; Incorrect charging for labour and material, misuse of assets or product substitution, including substituting a product for one of a lesser quality.
Tendering	Collusive tendering (the act of multiple tenderers for a particular contract colluding in the preparation of their bids); A UNE Representative manipulating a tendering process to achieve a particular outcome; Acceptance of a payment, gift or hospitality from a third party where it is known, or suspected (or should be suspected) that it is offered or provided with an expectation that a business advantage will be provided in return.
Credit Cards, EFTPOS, cheques	Using a University credit card for personal expenses and claiming them as University related; Unauthorised use of a credit card or a credit card issued to another person; Making or using forged or falsified document or signatures.
Procurement and accounts payable	Receiving kickbacks or secret commissions from a contractor; Misappropriating official order forms to gain a personal benefit; Making cheques out to false persons/ companies, etc; False invoicing involving a UNE Representative; A person external to the University creating a false invoice for payment by UNE, claiming payment for goods or services not delivered, or exaggerating the value of goods delivered or services provided.
Conflicts of Interest	A UNE Representative acting in their own self-interest rather than the interests of the University in relation to University matters; Failure to disclose and actual, perceived or personal conflict of interest contrary to the Code of Conduct and the Conflicts of Interest Policy; Allowing a conflict of interest to undermine independence; Nepotism and cronyism
People and Culture	Misuse of personal or sick leave; Failing to apply for leave taken when not working; Receiving personal benefits in exchange for assisting a consultant to gain work at the University; Payment of secret commissions to a UNE Representative that is related to a specific action or decision of the UNE Representative; Receiving kickbacks or secret commissions from a contractor; Submission of exaggerated, or wholly fictitious, or vexatious accident, harassment, bullying or injury claims.
Student Admission and Records	Evasion of fees due to the University; Making, using or possessing forged or falsified documents such as degrees, academic transcripts, testamurs and other academic records; Using forged or falsified documents when applying for admission, or advanced standing/ credit towards a course; Using forged or falsified documents when applying for special study accommodations, extensions of time; Submitting the work of others as if it were the students own work (Also Academic/ Research Misconduct).

Section 3 - Authority and Compliance

(57) The Council, pursuant to Section 29 of the University of New England Act 1993 (NSW) makes this University Policy.

(58) The Policy Steward, Director Governance and University Secretary (DGUS), is authorised the develop supporting documents to support this Policy.

(59) This Policy operates as and from the Effective Date.

(60) Previous policy and plans on fraud and corruption controls are replaced and have no further operation from the Effective Date of this Policy.

(61) Notwithstanding the other provisions of this Policy, the Vice-Chancellor and Chief Executive Officer may approve an exception to this Policy where the Vice-Chancellor and Chief Executive Officer determines the application of this Policy would otherwise lead to an unfair, unreasonable or absurd outcome. Approvals by the Vice-Chancellor and Chief Executive Officer under this clause must:

a. be documented in writing;
b. state the reason for the exception; and
c. be registered in the approved UNE electronic Records Management System (RMS) in accordance with the Records Management Rule.

Section 4 - Quality Assurance

(62) The implementation of this Policy will be supported and measured by UNE annually to ensure the level of understanding, engagement and application of this Policy meets expectations.

Status and Details

Status	Current
Effective Date	31st March 2023
Review Date	31st March 2024
Approval Authority	Audit and Risk Committee
Approval Date	28th February 2023
Expiry Date	Not applicable
Unit Head	Susannah Warrick Director Governance and University Secretary swarrick@une.edu.au
Enquiries Contact	Susannah Warrick Director Governance and University Secretary swarrick@une.edu.au Internal Audit +61 2 6773 4483

Glossary Terms and Definitions

"UNE Representative" - Means a University employee (casual, fixed term and permanent), contractor, agent, appointee, UNE Council member, adjunct, visiting academic and any other person engaged by the University to undertake some activity for or on behalf of the University. It includes corporations and other bodies falling into one or more of these categories.

"In Writing" - Means by letter, email or fax.

"Student" - Is an admitted student or an enrolled student, at the relevant time: 1. an admitted student is a student who has been admitted to a UNE course of study and who is entitled to enrol in a unit of study or who has completed all of the units in the UNE course of study; 2. an enrolled student is a student who is enrolled in a unit of study at UNE.

"Cost Centre" - Is the relevant Faculty, Directorate or other business unit.

"Senior Executive" - Means the Vice-Chancellor, Deputy Vice-Chancellor, Deputy Vice-Chancellor Research, Chief Financial Officer, and Chief Operating Officer.

"Personal Information" - Refers to information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. In accordance with Section 4 of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA). It includes such things as: a. a person's name, address, information about a person's family life, information about a person's sexual preferences, financial information, photos, contact details, opinions, health conditions or illnesses, housing or tenancy information, work history, education and criminal histories; b .an individual's fingerprints, retina prints, body samples or genetic characteristics; c. payroll details, information about next of kin, emergency contacts, superannuation fund and tax file numbers; d. health information, in accordance with Section 6 of the Health Records and Information Privacy Act 2002 (NSW), incorporating information or opinions about: the physical or mental health or a disability (at any time) of an individual, or an individual's express wishes about the future provision of health services to him or her, or a health service provided, or to be provided, to an individual, or other personal information collected to provide a health service, or in providing a health service, or in connection with the donation of human tissue or body parts; or genetic information that is or could be predictive of the health of a person or their relatives or descendants; and e. some things (such as information about an individual who

has been dead for more than 30 years and information about an individual that is contained in a publicly available publication) are exempt from the definition of "personal information" and these are listed in full, under Section 4(3) of the PPIPA.

"Conflicts of Interest" - A UNE Representative will have a conflict of interest where they have a material interest in a decision or matter, and/or their interest appears to raise a conflict with the proper performance of their duties (e.g. avoiding personal losses as well as gaining personal advantage — whether financial or otherwise).

"Risk Management" - Means coordinated activities to direct and control an organisation with regard to its management of corporate risk.

"Fraud" - Means an intentional act by one or more individuals involving the use of deception to obtain an unjust or illegal advantage.

"Records Management System (RMS)" - The University of New England installation of TRIM (Content Manager), or equivalent replacement system, under the control of the Records Management Office.

"Effective Date" - means the Rule/Policy takes effect on the day on which it is published, or such later day as may be specified in the policy document.

"Approval" - A statement to indicate the official acceptance of a proposal, recommendation, or other matter. It is a function of the role/committee with delegated authority to do so.

"Allegation" - An allegation is a claim or assertion that someone has done something illegal or wrong, typically one made without proof.

"Complaint" - A complaint is defined as a statement that something is unsatisfactory or unacceptable.