DATA AND RECORDS INTEGRITY POLICY AND PROCEDURES

Purpose

The secure maintenance of data integrity is a major priority for Lincoln Education Australia (LEA). Data and records are a critical strategic asset which are used to inform business administration decisions and ensure transparency and accountability of operations. Further, the majority of data held by LEA consists of highly confidential student records. LEA is thus committed to effectively managing all data and records to ensure that only individuals holding the correct authorisation have access.

The *Data and Records Integrity Policy and Procedures* outlines the principles and procedures involved in maintaining the integrity of data and records at LEA.

POLICY

Scope

This policy applies to all staff and students at LEA.

Principles

LEA creates and stores data in order to:

- Document business activities
- Ensure that practices are consistent by allowing staff access to prior student data and decisions made with regards to it
- Protect the rights of staff, students, and visitors
- Ensure that LEA can demonstrate compliance with all external regulatory requirements, including the HESF 2015 and ESOS Act.
- Maintain accountability for any business activities that are associated with staff, student, or other data.

Data integrity is a key element of decision-making and business practices, as well as accountability, transparency, and risk management at LEA. Key areas of data collection for these processes include:

- Critical incidents
- Allegations of misconduct
- Breaches of academic or research integrity
- Responses to each incident, and accountability for the response
- Institutional student data relating to retention, progression, and performance

Data may include:

- Digital or hard copy records
- Documents (print or electronic)

- Evidence of online activity including email
- Information stored on databases, including physical or online storage

Record keeping practices should be consistent, secure, and in line with Australian State and Commonwealth regulatory requirements. LEA recognises its obligations under the *Privacy Act 1988 (Cth)*.

PROCEDURES

Data Classifications

All data within LEA falls into one of the following categories:

- Public data
- Internal data
- Internal protected data
- Internal restricted data

Data Security and Storage

All data shall be secured in order to:

- Ensure integrity and authenticity,
- Prevent access except by authorised parties,
- Prevent removal or alteration of data.

All data shall be stored for seven years, at which point it may either be archived or disposed. If records and data are deemed to be of future value to LEA, either to inform decisions or demonstrate compliance, they are to be archived.

All internal data is tobbe stored with security measures appropriate to its category of confidentiality. All internal physical data shall be stored in locked metal filing cabinets, while all internal digital data is to be stored in a password-protected database that is regularly backed up and access granted only to personnel with written approval of the IT Manager and the COO.

The categories of data are defined as follows:

Public Data

Public access data is to be freely available to both members of the LEA community, and the general public. Public data includes but is not limited to course information, enrolment dates, and LEA contact details. The Marketing Manager in liaison with the IT Manager are responsible for ensuring that all public data is up-to-date and publicly accessible.

Internal Data

Internal data is available to LEA 's administrative staff for use. Internal data includes LEA staff policies, work meeting minutes, and other work-related documents. The Chief Operating Officer (COO) is responsible for ensuring that all internal data is only available to the relevant staff members of the LEA.

Internal Protected Data

Internal protected data is only accessible by selected authorised staff. Internal protected data includes student assessment outcomes, student examinations, and academic staff research. The Corporate Governance Board and Dean (where the data relates to student information) are responsible for ensuring that adequate security measures are in place to prevent unauthorised parties from accessing LEA 's internal protected data.

Internal Restricted Data:

Information that is classified as internal restricted data is to be treated with the utmost confidentiality, with access limited to staff at the highest levels of operations. Internal restricted data includes but isn't limited to formal complaints and allegations of misconduct, contracts and commercial-in-confidence records, critical incident reports, records of alleged breaches of academic or research integrity, records of responses to the aforementioned instances, as well as who is responsible for the responses. The Corporate Governance Board and Chief Operating Officer (if the data relates to student information) are responsible for implementing the necessary security measures to prevent unauthorised access.

Student Records

Student records are a critically important category of sensitive data that LEA keeps. This involves records such as:

- Student contact details
- Biographical information, including date of birth
- Applications
- Finance information
- Visa information (if applicable)
- Grades and progression
- Completions and award of qualifications
- Complaints and appeals
- Instances of misconduct (including allegations)
- Breaches of academic or research integrity
- Critical incidents relating to the student.

Student records are created and kept for the purposes of:

- Various enrolment, academic, and administrative processes.
- Course development.

- Improvement of operations and processes such as the complaints and appeals channels, admissions, and support services.
- Ensuring that the rights of all LEA staff, students, and visitors are protected.
- Ensuring LEA is held accountable for any business activities that are affiliated with student records.

All student information is be appropriately organised; this is the joint responsibility of the IT staff, student administrative staff, and Academic Dean.

All student information is to be treated as digital internal protected or restricted data depending on its nature and is to be protected in accordance with the level of security and access restrictions defined above. Information may also be released in the following extenuating circumstances:

- A parent or legal guardian of a student under the age of 18 provides a written request for access to the information.
- LEA receives a judicial order requiring access to the information.

Data Access

Staff are authorised to access data based on their position in LEA. Internal data is not to be disclosed by authorised students and staff to unauthorised parties.

If a student has a query regarding authorisation for access to information, they should consult student support services.

If a staff member has a query regarding authorisation for access to information, they should consult their supervisor.

If a staff member needs to be granted increased clearance to access records or data (such as when a staff member is appointed to a more senior role), a request shall be submitted in writing to the relevant supervisor in charge of maintaining those records. The request shall have the sign-off of the IT Manager and COO in order for the request to be granted.

All members of the LEA community are expected to comply with the level of access they are granted and report any breaches they witness or engage in.

Updating Data

All data held by LEA is expected to be accurate and up to date.

All staff and students at LEA are required to notify administration staff if the need for updating data comes to their attention.

Disposing of Data

Data is to be disposed of confidentially and the reason for disposal to be recorded. Records shall not be disposed of if:

- They have been active in the last 6 years
- There are current tasks or procedures that require their use
- They have been archived

In order to dispose of documents containing student information, specific procedure shall be followed:

- The document is to be verified to determine it is a copy or if it is the original document.
- If the document is an original document, its content shall be identified and assessed by the appropriate authority and its relevance determined.
- If the document is determined to no longer be of relevance, a submission to the Corporate Governance Board regarding the disposal of the document is to be made and upon approval, the document disposed of in an appropriate manner that ensures the confidentiality of student information is maintained.
- Reasons explaining why the document was disposed at to be archived.

Responsibilities

As part of new staff induction, LEA staff are to be made aware of their responsibilities for ensuring data integrity. These responsibilities include:

- Adhering to the procedures outlined in the *Data and Records Integrity Policy and Procedures* and any additional instructions received from supervisors
- Creating accurate records of LEA activities
- Ensuring, to the best of their ability, that all data is authentic
- Updating and archiving data wherever necessary
- Reporting any misconduct that comes to their attention.

In addition to general staff responsibilities, supervisors shall ensure that they:

- Train staff in their roles and responsibilities relating to data integrity
- Oversee staff recordkeeping to maintain proper capture, management, and security of data, including staff and student records
- Document procedures for capturing and preserving student and staff records and other data
- Work to oversee record keeping systems, storage and disposal, and improve data integrity practices
- Maintain oversight of which staff members are authorised to access student and staff data.

Breaches

Breaches of the *Data and Records Integrity Policy and Procedures* represent a major risk to LEA and are to be responded to with utmost seriousness. Disciplinary action may be taken against any member of the LEA community who breaches or attempts to breach this policy. Referral to law enforcement will occur if policy breaches result in financial loss for LEA or the compromise of its students' privacy.

For any suspected breach of this policy, a full investigation and hearing may be undertaken. The information collected during this process shall be used by the Corporate Governance Board to plan preventative measures for future breaches of data integrity.

Compliance

All staff and students at LEA are required to comply with this policy and its procedures, and with related policies and respective procedures. Non-compliance may result in a disciplinary action.

File Number	LEA-GEN-COR-70025-D
Responsible Officer	Chief Executive Officer
Contact Officer	Chief Operating Officer
Legislative Dompliance	• *Higher Education Standards Framework (Threshold Standards) 2015* • *Privacy Act* 1988 (Cth) • *Tertiary Education Quality and Standards Agency Act 2011*
Supporting Documents	
Related Documents	• *Degree Issuance and Replacement Policy and Procedures* • *Information for Students Policy and Procedures*
Superseded Documents	
Effective Date	1 January 2022
Next Review	3 years from the effective date

Definitions

Corporate Governance Board: Governing body responsible for oversight of all higher education operations, including the ongoing viability of the institution and the quality of its higher education delivery. The Corporate Governance Board guides the Management and delegates responsibility for academic matters to the Academic Board.

Chief Executive Officer (CEO): Head of the executive management team responsible for the management of the day-to-day operations of LEA, its people and resources.

Chief Operating Officer (COO): Provides leadership and management of the operations of LEA, coordinates the implementation of programs and campus collaboration, within the broad parameters of LEA's strategic directions.

Academic Dean: Responsible for the academic standards of LEA and for maintaining and developing academic courses, teaching excellence and interaction with stakeholders. Provides leadership within the broad parameters of LEA's strategic directions, and plays a crucial role in defining, disseminating and supporting academic standards and values across LEA.

Student Records: Records that contain evidence or information about a student's undertakings during their period of enrolment at LEA University. Students records include, but are not limited to, course applications and supporting documentation, examination records, personal details, assessments, and academic transcripts.

Review

This policy shall be reviewed by the Corporate Governance Board every 3 years.

Version History			
Version number:	Approved by:	Approval Date:	Revision Notes:
1.0	Corporate Governance Board	17/12/2020	New policy