Data and Records Integrity Policy

Version number	2
Approved by	Corporate Governance Board
Date of approval	29/07/2020

Purpose

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

This policy outlines the principles and procedures involved in maintaining the integrity of data and records at SI as well as SI's commitment to maintaining information privacy.

Scope

This policy applies to all staff and students at SI.

Principles

SI 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 in regard to it
- Protect the rights of staff, students, and visitors
- Ensure that SI 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 SI. 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 federal regulatory requirements and *General Retention and Disposal Authority: University Records (GDA23)*. SI recognises its obligations under the *Privacy Act 1988 (Cth)*.

Procedures

Data Classifications

All data within the SI will fall into one of the following categories:

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

Data Security and Storage

All data must be secured in order to:

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

All data will be stored, archived or disposed of in accordance with *General Retention and Disposal Authority: higher & further education and research records (GDA45)*. If records and data are deemed to be of future value to SI, either to inform decisions or demonstrate compliance, they must be archived.

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

The categories of data are defined as follows:

Public data

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

Internal data

Internal data is available to the SI's administrative staff for use. Internal data includes SI staff policies, work meeting minutes, and other work-related documents. The Provost is responsible for ensuring that all internal data is only available to the relevant staff members of the SI.

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 Provost (where the data relates to student information) are responsible for ensuring that adequate security measures are in place to prevent unauthorised parties from accessing the SI's internal protected data.

Internal restricted data:

Information that is classified as internal restricted data will 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 health-related information, 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 Provost (if the data relates to student information) will be responsible for implementing the necessary security measures to prevent unauthorised access.

Student Records

Student records are a critically important category of sensitive data that SI 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.
- Program development.
- Improvement of operations and processes such as the complaints and appeals channels, admissions, and support services.
- Ensuring that the rights of all SI staff, students, and visitors are protected.
- Ensuring the SI is held accountable for any business activities that are affiliated with student records.

All student information will be appropriately organised and protected; this will be the joint responsibility of the SI's IT staff, professional staff, and Provost.

All student information will be treated as digital internal protected or restricted data depending on its nature and will 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.
- SI receives a judicial order requiring access to the information.

Data access
Staff are authorised to access data based on their position in SI.

Internal data is not to be disclosed by 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 must be submitted in writing to the relevant supervisor in charge of maintaining those records. The request must have the sign-off of the IT Coordinator and Provost in order for the request to be granted.

All members of the SI 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 within the SI is expected to be accurate and up to date.

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

Disposing of data

Data will be disposed of confidentially and the reason for disposal will be recorded in accordance with *General Retention and Disposal Authority: University Records (GDA23)*.

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

- The document must be verified to determine it is a copy or if it is the original document.
- If the document is an original document, its content must be identified and assessed by the appropriate authority and its relevance determined.
- If the document is determined to no longer be of relevance, the Provost will approve the disposal and the documents will be disposed of in an appropriate manner that ensures the confidentiality of student information is maintained.
- Upon disposal, reasons explaining why the document was disposed of must be archived.

Responsibilities

As part of new staff induction, SI staff will 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 any additional instructions received from supervisors
- Creating accurate records of SI 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 must 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* represent a major risk to SI and will be responded to with utmost seriousness. Disciplinary action may be taken against any member of the SI community who breaches or attempts to breach this policy. Referral to law enforcement will occur if policy breaches result in a financial loss for the SI or compromise its students' privacy.

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

Policy Implementation and Monitoring

The *Corporate Governance Board* delegates responsibility for the day-to-day implementation of this policy to the Provost and other positions specified in 'Procedures' above.

The *Corporate Governance Board* will review all periodic reports from relevant committees and staff members, in accordance with the *Compliance Calendar*.

Additionally, the *Corporate Governance Board* will review all relevant student complaints, concerns raised by staff members, and instances of student or staff misconduct in accordance with the *Compliance Calendar*.

The *Corporate Governance Board* must ensure that findings from these monitoring activities are taken into account in planning, quality assurance and improvement processes.

Related documents

- *Privacy Act 1988 (Commonwealth)*
- *General Retention and Disposal Authority: higher & further education and research records (GDA45)*

Definitions

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

SI Community: Consists of staff, students and other stakeholders of SI.

Review schedule

This policy will be reviewed by the *Corporate Governance Board* every three years.

Version History				
Version number:	Approved by:	Approval date:	Revision notes:	Next review date:
1	Corporate Governance Board	13/11/2017		13/11/2020
2	Corporate Governance Board	29/07/2020	Replace GA36 standard with GA45	29/07/2023

Related Documents

	Degree Issuance and Replacement Policy
	Information For Students Policy
	Provost
	Marketing and Communications Coordinator
	IT Coordinator
	Corporate Governance Board – Terms of Reference

End of document: "Data and Records Integrity Policy"
Document ID: 8581, **Revision No : (10), Created :** January 6, 2020 11:01 am, **By :** Aleisha Zhao, **Last updated :** July 28, 2020 1:40 pm, **Updated by :** Nigel Finch, **Reviewed & Approved by :** Nigel, **On :** January 1, 1970, **Next Review by :** Nigel, **Review Scheduled For :** January 1, 1970
Produced & Printed : Thursday 10th of September 2020 03:02:55 AM "Sydney Institute of Higher Education ABN 49 618 742 813 TEQSA PRV14323 CRICOS 03866C"