RECORDS MANAGEMENT POLICY

1. Purpose

1.1 Ikon's records provide evidence of actions and decisions and represent a vital asset to support its daily functions and operations

1.2 This policy outlines the principles and procedures involved in maintaining the integrity of data and records at Ikon, to ensure that records are retained, maintained, and secured in accordance with legislation to safeguard the privacy of personal and sensitive information of individuals whilst maintaining the appropriate records of the educational activities of Ikon.

2. Scope

2.1 This policy covers all personal and sensitive information relating to students and staff and all institutional records including educational, training, assessment, policy, financial, IP, compliance, and quality documents.

3. Related Documents

This policy should be read in conjunction with the following documents:

- Privacy Policy
- Governance Guidelines
- Grievance and Appeals Policy
- Policy Framework
- Compliance Framework Policy
- Compliance Register
- Domestic Student Admission Policy
- International Student Admission Policy
- Student Academic Progress Policy
- Inclusion, Diversity and Equity Policy

This policy and related documents can be accessed via the *Policy and Procedures* section of the Ikon website, and/or the student and staff policy libraries.

4. Definitions

"Business Records" means any current or former financial, administration, governance, and all other records that are not student or staff related.

"Data" includes:

- digital or hard copy records
- documents (print or electronic)
- evidence of online activity including email
- information stored on databases, including physical or online storage

“**Student Personal Information**” means personal information and includes assignments, examinations, individual student results, student results collated in a list with identification by student number, and practicum, field and clinical placement details, financial details, emergency contact details. This definition is in accordance with the definitions in the *Privacy Act 1988* and the *Higher Education Support Act 2003.*

“Staff Personal Information” means personal details, contact details, payroll details, qualifications, employment history, performance reviews, and complaints**.**

“**Sensitive Information**” means personal information about an individual's racial or ethnic origin, political opinion, membership of a political association, religious beliefs or affiliations, health status (either physical or emotional), disability, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, or criminal record.

“Student Records” means records that contain evidence or information about a student’s undertakings during their period of enrolment at Ikon, and include course applications and supporting documentation, assessment records, personal details, assessments, and academic transcripts.

POLICY

5. Principles

5.1 Ikon is committed to maintaining the security of personal and sensitive information and to safeguarding institutional and personal records. The policy is based on the following principles:

- the interests of the individual and the preservation of their privacy and confidentiality are paramount.
- the principle of minimal disclosure shall be applied to all areas of academic and administrative practice.
- students and staff have a right to know how their personal information shall be managed, including the use, storage and disposal and disclosure of that information.
- students and staff have a right to know the personal information that is held about them and to correct such information as required.
- information kept shall be up-to-date and accurate, and only used only for the purposes for which it is acquired.
- information shall not be disclosed to others (including parents, friends, and spouses) without written permission from the individual concerned.
- student information shall not be disclosed to staff unless they are directly involved with student results and student welfare.
- information shall be disclosed to Federal and State authorities as required under legislation.
- all student records shall be held securely and backed up at an off-site location.
- the preferred method of record keeping is by electronic means.

5.2 Ikon 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 Ikon can demonstrate compliance with all external regulatory requirements, including the HESF 2021 and the National Code 2018.
- maintain accountability for any business activities that are associated with staff, student, or other data.

5.3 Data integrity is a key element of decision-making and business practices, as well as accountability, transparency, and risk management at Ikon. 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

5.4 Record keeping practices shall be consistent, secure, and in line with Australian State and Commonwealth regulatory requirements, including the *Privacy Act 1988 (Cth)*.

6. Roles & Responsibilities

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

- adhering to the procedures outlined in this policy and any additional instructions received from supervisors or senior staff
- creating accurate records of Ikon 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

6.2 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 what student and staff data.

PROCEDURE

7. Maintaining Records

7.1 Staff shall record personal information of students on enrolment which may be held in digital format or on paper records.

7.2 Staff shall record all changes to personal information as received and all aspects of assessment and academic achievement, and all student fee payments and details of any refunds paid.

7.3 Manual student records shall be kept securely in a lockable cabinet.

7.4 Student records shall use the Wisenet Student Administration System. The safety features of this system are outlined in Wisenet's Data Safety and Security documents.

7.5 Electronic records shall be regularly backed up (weekly) and archived. Aged files are to be archived and stored in secure facilities.

7.6 Ikon shall request and hold the minimum personal data necessary to enable it to perform its function and it shall not hold it for longer than necessary than the purpose for which it was collected.

7.7 Every effort shall be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

8. Data Security and Storage

8.1 All data within Ikon falls into one of the following categories:

- public data
- internal data
- internal protected data
- internal restricted data

8.2 All data shall be secured in order to:

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

8.3 To enable the issuance of replacement testamurs and academic transcripts, student records of achievement shall be held securely indefinitely or as otherwise as required by legislation.

8.4 Records of course and subject reviews shall be stored in order to meet auditing requirements and timeframes of the registering and accrediting agencies and the *Higher Education Support Act 2003*.

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

8.6 All internal data is to be 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 CEO.

8.7 The categories of data are defined as follows:

Public Data

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

Internal Data

8.9 Internal data is available to administrative staff for use and includes staff policies, meeting minutes, and other work-related documents. The CEO is responsible for ensuring that all internal data is only available to relevant staff members.

Internal Protected Data

8.10 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 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 Ikon's internal protected data.

Internal Restricted Data:

8.11 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. 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. The Corporate Board and the Dean (if the data relates to student information) are responsible for implementing the necessary security measures to prevent unauthorised access.

9. Data Safety and Confidentiality

9.1 Ikon shall ensure that the information network is as safe and secure as reasonably possible and that the procedures approved within this policy are implemented. The security of Ikon's information systems shall be reviewed regularly including regular updates of virus protection.

9.2 User logins and passwords are required to access Ikon's network. Members of staff shall not, as a matter of course, be granted access to the whole management information system and shall only be granted access permissions in line with the role requirements.

9.3 Staff shall maintain privacy and shall not give passwords to others.

10. Student Records

10.1 Student records are a critically important category of sensitive data that Ikon 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.

10.2 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 Ikon staff, students, and visitors are protected.
- ensuring Ikon is held accountable for any business activities that are affiliated with student records.

10.3 A copy of testamurs, records of results, academic transcripts and statements of attainment shall be electronically kept in the student's academic file

10.4 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.
- Ikon receives a judicial order requiring access to the information.

11. Data Access

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

11.2 If a student has a query regarding authorisation for access to information, they should consult the Student Experience Team.

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

11.4 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), the request shall have the sign-off of the CEO in order for the request to be granted.

11.5 All members of the Ikon community are expected to comply with the level of access they are granted and to report any breaches they witness or engage in. Any breaches are to be reported to the Quality Assurance Manager.

12. Updating Data

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

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

13. Published Content

13.1 Editorial guidance from marketing shall ensure that Ikon's ethos is reflected on the Ikon website, and that information is accurate and personal security is not compromised.

13.2 Staff and students' personal information shall not be published on the website.

13.3 Photographs that include Ikon students shall be carefully selected and shall not enable individual students to be clearly identified by members of the public viewing the website. Students' full names shall not be used anywhere on a website or blog, particularly in association with photographs. In the event photographs or testimonials that can identify students are desired for marketing purposes, direct written permission shall be sought from the student.

14. Student Access to Personal Records

14.1 A student who wishes to apply for and receive personal information that the Ikon holds about them is required to:

- make a written application to the Registrar.
- the Registrar shall give written notice of receipt of the application within five (5) working days of its lodgement.
- within ten (10) working days of the lodgement of the application, the Registrar shall provide the requested information in writing.

15. Correcting a Student Record

15.1 Where a record is found to be inaccurate, a student may request in writing that a correction be made, citing details that need to be corrected and providing the correct information and any supporting information.

15.2 The Registrar shall give written notice of receipt of the request for correction within five (5) working days of receiving the request.

15.3 Within ten (10) working days of the lodgment of the notice, the Registrar shall make the necessary corrections to Ikon records and provide the student with confirmation in writing that the requested corrections have been made.

15.4 Where a student requests that a record be amended because it is inaccurate but the record is found to be accurate, the details of the request for amendment shall be noted on the record and the student shall be advised in writing.

16. Staff Records and Access to Records

16.1 Designated Ikon staff shall maintain up to date records of the contact details, employment history and qualifications of all staff employed by Ikon.

16.2 Staff have a right to know the personal information that is held about them and to correct such information as required.

16.3 Staff, as described in their position description, shall have access to records solely for the purposes of their job.

17. Disposing of Data

17.1 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

17.2 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 Board of Directors 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.

18. Breaches

18.1 Breaches of this policy represent a major risk to Ikon and are to be responded to with utmost seriousness. Disciplinary action may be taken against any member of the Ikon community who breaches or attempts to breach this policy. Referral to law enforcement will occur if policy breaches result in financial loss for Ikon or compromises the privacy of students and staff.

18.2 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 Board to plan preventative measures for future breaches of data integrity.

18.3 All breaches are to be recorded in the *Compliance Register*.

19. Grievances

19.1 Where a student has a grievance or complaint in relation to a decision made pursuant to this policy, they may avail themselves of Ikon's grievance procedures outlined in the *Grievance & Appeals Policy.*

19.2 Where a staff member has a grievance or complaint in relation to a decision made pursuant to this policy, they should contact their immediate supervisor or the HR Manager.

20. Cessation of Business

21.1 In the case that Ikon should cease its services and the discontinuation of its business the CEO shall ensure that all student records are made available to the relevant Federal and State authorities.

21. Publication

22.1 This policy shall be published in the *Policy and Procedures* section of the Ikon website, and the student and staff policy libraries.

Policy Information & History

Policy Category	Corporate, Governance
Policy ID	GO012A
Approved by	Board of Directors
Date of Approval	4 March 2022
Previous Versions	9 February 2016, 30 May 2011, 2 March 2009, 1 April 2005
Next Review Date	March 2025
Government Legislation	Tertiary Education Quality and Standards Agency Act 2011 Higher Education Support Act 2003 Higher Education Standards Framework (Threshold Standards) 2021 National Code 2018 Privacy Act 1988 Freedom of Information Act 1982
Responsible Officer	CEO
Sources:	In developing this policy, the following documents were considered: Department of Education, Skills and Employment, I*mproving Transparency and Accountability: Student Records Management,* 18 June 2020
Benchmarking:	External referencing activities were conducted against comparable providers and best practice using publicly available information, including: Kaplan Business School, University of Technology Sydney, Western Sydney University, University of South Australia, and James Cook University.