	Business Manual Policy	
	No: 01.02.	Rev: 1
	Recordkeeping & Data Privacy Policy	
THIS DOCUMENT SUPERSEDES XXX. ALL REFERENCES TO SUPERSEDED DOCUMENTS MUST NOW BE READ AS THIS DOCUMENT NUMBER.		

Record keeping & Data Privacy Policy

Overview

This policy has been designed to ensure that Elevare International Institute maintain accurate, secure, and lawful records of student and staff information, in compliance with the Privacy Act 2020 (NZ), the Privacy Act 1988 (AU), and relevant education regulatory frameworks.

SCOPE

This policy applies to all personal, academic, financial, and operational records created, stored, accessed, or disposed of by the organisation, including physical and digital formats.

APPLICABILITY

This document is applicable to the following areas:

☒ All Company Activities

ABBREVIATIONS

ABBR	Meaning
BM	Business Manual
OSHC	Overseas Student Health Cover
IAW	In Accordance With

DEFINITIONS

Term	Meaning
Policy	Deliberate statement of intent pertaining to a specific function within School of Business Ltd.


	Business Manual Policy	
	No: 01.02.	Rev: 1
	Recordkeeping & Data Privacy Policy	
THIS DOCUMENT SUPERSEDES XXX. ALL REFERENCES TO SUPERSEDED DOCUMENTS MUST NOW BE READ AS THIS DOCUMENT NUMBER.		

TABLE OF CONTENTS

Overview1

SCOPE..1

APPLICABILITY1

ABBREVIATIONS1

1. Principles4


2. Record Types.....4

3. Data Storage & Security4

4. Access & Disclosure4

5. Retention & Disposal4

6. Breach Management4

	Business Manual Policy	
	No: 01.02.	Rev: 1
	Recordkeeping & Data Privacy Policy	
THIS DOCUMENT SUPERSEDES XXX. ALL REFERENCES TO SUPERSEDED DOCUMENTS MUST NOW BE READ AS THIS DOCUMENT NUMBER.		

REFERENCE DOCUMENTATION

EXTERNAL AND INTERNAL NON FEBM DOCUMENTATION

	Document Reference	Document Title
[1]		Privacy Act 2020
[2]		NZQA Code of Practice 2021
[3]		Education Act 1989
[4]		

RELATED BM POLICIES AND PLANS

	BM Number	Document Title	Previous Number(s)
[5]	01.02.	Privacy & Confidentiality Policy	
[6]	01.02.	Student Enrolment Policy	
[7]	01.04.	Doe of Practice Implementation Plan	
[8]			

RELATED BM PROCEDURES AND INSTRUCTIONS

	BM Number	Document Title	Previous Number(s)
[9]	01.03.	Complaints and Grievances Procedure	
[10]			

RELATED BM FORMS

	BM Number	Document Title	Previous Number(s)
[11]	01.05.	Data Access Request Form	
[12]	01.05.	Privacy Breach Register	
[13]	01.05.	Staff Confidentiality Agreement	
[14]			



Business Manual Policy

No: 01.02.

Rev: 1

Recordkeeping & Data Privacy Policy

THIS DOCUMENT SUPERSEDES XXX. ALL REFERENCES TO SUPERSEDED DOCUMENTS MUST NOW BE READ AS THIS DOCUMENT NUMBER.

1. Principles

- **Lawful Collection:** Data is collected for legitimate educational, operational, and compliance purposes.
- **Informed Consent:** Individuals are informed of data collection and provide consent where required.
- **Secure Storage:** Records are stored securely to prevent unauthorized access, loss, or misuse.
- **Limited Access:** Access is restricted to authorized personnel based on role and necessity.
- **Retention & Disposal:** Records are retained for the required period and disposed of securely.
- **Transparency & Access:** Individuals may request access to or correction of their personal data.
- **Audit Readiness:** Records are maintained in a format suitable for internal and external audit.

2. Record Types

Record Type	Examples	Retention Period
Student Records	Enrolment forms, academic results, attendance logs	7 years post-completion
Staff Records	Contracts, performance reviews, training logs	7 years post-employment
Financial Records	Invoices, receipts, funding documentation	7 years
Governance Records	Board minutes, strategic plans, compliance reports	Permanent or as per legal requirement
Incident Records	Complaints, breaches, investigations	7 years or until resolved

3. Data Storage & Security

- All digital records are stored in secure, access-controlled systems (e.g., SMS/LMS, cloud platforms).
- Physical records are stored in locked cabinets with restricted access.
- Backups are performed regularly and stored offsite or in secure cloud environments.
- Staff must complete annual data privacy training.

4. Access & Disclosure

- Access to records is role-based and logged.
- Disclosure to third parties requires written consent, unless legally mandated.
- Students and staff may request access or correction via the **Data Access Request Form**.

5. Retention & Disposal

- Records are retained in accordance with legal and regulatory requirements.
- Disposal is conducted via secure shredding (physical) or certified digital deletion.
- Disposal actions are logged in the **Data Disposal Register**.

6. Breach Management

- Suspected breaches must be reported immediately using the **Privacy Breach Incident Report**.
- The **Privacy Officer** will investigate and report outcomes to the Governance Board.
- Serious breaches may be reported to the Office of the Privacy Commissioner (NZ) or OAIC (AU).