MortarCAPS Higher Learning Data Standard Ltd

Information Security Policy

Organisation	MortarCAPS Higher Learning Data Standard Ltd (ACN 684 569 864)
Registered address	368 Sussex Street, Sydney, NSW 2000, Australia
Policy owner	Gemma Williams, Head of Operations
Approved by	Board of Directors
Version	1.0
Effective date	17 February 2025
Next review	February 2027

1. Purpose

MortarCAPS Higher Learning Data Standard Ltd relies on information and information systems to deliver its charitable purpose, including the handling of higher-education data. This policy establishes the framework for protecting the confidentiality, integrity and availability of information held or processed by the Organisation.

2. Scope

This policy applies to all directors, employees, volunteers, contractors and third parties who access the Organisation's information, systems or networks, and to all information assets regardless of format or location.

3. Legislative and standards framework

This policy is made having regard to:

- **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)**
- the **Notifiable Data Breaches (NDB) scheme** under Part IIIC of the Privacy Act
- **Privacy and Personal Information Protection Act 1998 (NSW)** where applicable
- ACNC Governance Standard 3 (acting lawfully), and
- the principles of **ISO/IEC 27001** as a framework for information security management.

4. Security principles

- **Access control:** Access to information is granted on a least-privilege, need-to-know basis, with multi-factor authentication required for privileged and remote access.
- **Data classification and handling:** Information is classified and handled according to its sensitivity, with particular care for personal and sensitive information.
- **Encryption:** Data is encrypted in transit and at rest where appropriate.
- **Asset and supplier management:** Information assets are recorded and third parties are subject to proportionate due diligence and contractual security obligations.
- **Awareness:** All personnel receive information security and privacy awareness training.

- **Monitoring:** Access to and activity within systems is logged and monitored proportionate to risk.

5. Personal information and privacy

The Organisation collects, uses, discloses and stores personal information in accordance with the Australian Privacy Principles. Personal information is collected only for lawful purposes connected with our functions, kept secure, and retained no longer than necessary. Individuals may request access to, or correction of, their personal information.

6. Incident and data breach management

Suspected or actual information security incidents must be reported immediately to the policy owner. The Organisation maintains an incident response process covering classification, escalation, investigation, containment, remediation and lessons learned. Where an eligible data breach is likely to result in serious harm, the Organisation will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as required under the NDB scheme, without undue delay.

7. Business continuity

Backups, disaster recovery and business continuity arrangements are maintained proportionate to the criticality of systems and data, and are tested periodically. This policy operates alongside the Organisation's Business Continuity Plan.

8. Responsibilities and review

The Board approves this policy. Management implements and enforces controls. All users must comply with this policy and report concerns. This policy will be reviewed at least annually, with the next review due February 2027.

Approval

This policy has been approved by the Board of Directors of MortarCAPS Higher Learning Data Standard Ltd and is owned by the Head of Operations.

Signed: 

Gemma Williams
Head of Operations
MortarCAPS Higher Learning Data Standard Ltd

Date: 17 February 2025