Privacy Policy

How MortarCAPS collects, uses, protects and discloses personal information

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
Status	Final — published
Effective date	22 July 2026
Next review	July 2027 (annual)
Governing law	Privacy Act 1988 (Cth) and the Australian Privacy Principles

1. Our commitment and the law that applies

MortarCAPS Higher Learning Data Standard Ltd ("MortarCAPS", "we", "us") is committed to protecting your privacy. We handle personal information in accordance with the **Privacy Act 1988 (Cth)** ("the Privacy Act") and the thirteen Australian Privacy Principles (APPs) contained in Schedule 1 to that Act. This Privacy Policy explains what personal information we collect, how we use, disclose, secure and retain it, how we respond to data breaches, and how you can access, correct or complain about our handling of your information.

This policy should be read together with our Privacy Collection Notice, our Data Governance & Retention Policy and our Data Breach Response Plan.

2. Scope

This policy applies to all personal information MortarCAPS collects and holds, in any format or system, including information about:

- enquirers, subscribers and website visitors;
- representatives of member and partner institutions, vendors and contractors;
- individuals whose data forms part of the Human Capability Record (HCR); and
- our directors, staff and contractors.

3. Privacy contact (Privacy Officer)

We have appointed a named privacy contact who is responsible for privacy matters, access and correction requests, and complaints:

Privacy Officer	Gemma Williams, Head of Operations
Email	hello@mortarcaps.org
Post	Privacy Officer, MortarCAPS Higher Learning Data Standard Ltd, 368 Sussex Street, Sydney, NSW 2000, Australia

4. What personal information we collect

Consistent with APP 3, we collect only the personal information reasonably necessary for our functions and activities. This may include:

- identity and contact details — name, organisation, role, email, phone and postal address;

- correspondence and enquiry content you provide;
- programme and event participation records;
- HCR learner data, where an institution or learner provides it under the relevant consent arrangements; and
- website and technical data such as IP address and analytics collected automatically.

We do not collect sensitive information unless it is reasonably necessary and you have consented, or the collection is otherwise permitted under the Privacy Act.

5. How and why we collect and use it

We collect personal information directly from you (for example, when you contact us or subscribe), from partner institutions, and automatically through our website. Consistent with APP 6, we use personal information to:

- respond to your enquiry and provide requested information;
- administer our membership, partner and community programmes;
- develop and maintain the MortarCAPS Data Standard (MCDS) and the HCR;
- send updates you have asked to receive; and
- meet our legal, governance and reporting obligations.

We do not sell your personal information, and we do not use it for purposes unrelated to those above without your consent or as otherwise permitted by law.

6. Disclosure of personal information

We may disclose personal information to our service providers (such as hosting, email, analytics and professional advisers), to member and partner institutions where relevant to a programme, and where disclosure is required or authorised by law. Service providers are bound by confidentiality and privacy obligations equivalent to our own.

7. Cross-border disclosure (including Canada and New Zealand)

MortarCAPS operates and works with member institutions and vendors in Australia, New Zealand and **Canada**, and uses service providers that may store or access data overseas. As a result, your personal information may be disclosed to, or accessed from, recipients located outside Australia — including in **Canada** and New Zealand.

Before disclosing personal information overseas, we assess the transfer against **Australian Privacy Principle 8 (APP 8)** and take reasonable steps to ensure the overseas recipient handles the information consistently with the APPs. Where personal information is disclosed to or handled in Canada, additional laws may apply to the recipient, including Canada's **Personal Information Protection and Electronic Documents Act (PIPEDA)** and provincial laws such as **Quebec's Law 25**. Where information is handled in New Zealand, the **Privacy Act 2020 (NZ)** may apply.

Further detail on how we manage cross-border transfers is set out in our Data Governance & Retention Policy.

8. Data quality, security and retention

We take reasonable steps to keep personal information accurate, up to date and secure (APP 10 and APP 11), including access controls on a least-privilege, need-to-know basis, and to protect it from misuse, interference, loss and unauthorised access. We retain personal information only for as long as it is needed for the purposes described in this policy or as required by law, after which it is securely deleted or de-identified. Our standard retention periods are:

Information type	Retention period
Enquiry / contact data	2 years after last contact
Partner / licence records	7 years after end of agreement
Financial records	7 years
HCR learner data	For as long as consent is maintained and as required by applicable law; deleted on withdrawal of consent, subject to legal holds
Website / technical logs	Up to 12 months, unless required for a security investigation

Full detail is set out in our Data Governance & Retention Policy.

9. Notifiable data breaches

MortarCAPS complies with the **Notifiable Data Breaches (NDB) scheme** under Part IIIC of the **Privacy Act 1988 (Cth)**. If we suspect a data breach involving personal information, we follow our Data Breach Response Plan:

- **Contain** — we take immediate action to limit the breach;
- **Assess** — we assess, within 30 days, whether the breach is likely to result in serious harm to any individual;
- **Notify** — if serious harm is likely and the risk cannot be remediated, we notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as practicable, describing the breach, the information involved and recommended steps; and
- **Review** — we conduct a post-incident review and improve our controls.

All breaches and suspected breaches are recorded in our breach register, whether or not notification is required. Where a breach involves personal information from Canada or New Zealand, additional obligations under PIPEDA (including Quebec's Law 25) or the Privacy Act 2020 (NZ) may also apply.

10. Accessing and correcting your information

Under APP 12 and APP 13 you may request access to the personal information we hold about you and ask us to correct it if it is inaccurate, out of date, incomplete, irrelevant or misleading. To make a request, contact our Privacy Officer (section 3). We will respond within a reasonable period, ordinarily within 30 days, and will not charge an excessive fee. If we refuse access or correction, we will give you written reasons and information about how to complain.

11. How to make a privacy complaint

If you believe we have breached the Privacy Act or the Australian Privacy Principles, you can make a complaint using the following steps:

- **Step 1 — Contact us.** Send your complaint to our Privacy Officer at hello@mortarcaps.org, or by post to the address in section 3. Please describe the issue and how you would like it resolved.
- **Step 2 — Acknowledgement.** We will acknowledge your complaint within 5 business days.
- **Step 3 — Investigation and response.** We will investigate and provide a written response, ordinarily within 30 days.
- **Step 4 — External review.** If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (OAIC).

Office of the Australian Information Commissioner (OAIC)
Phone: 1300 363 992 | Online: www.oaic.gov.au | Post: GPO Box 5218, Sydney NSW 2001

12. Website, cookies and analytics

Our website may use cookies and similar technologies to operate the site and understand how it is used. You can manage cookies through your browser settings. Analytics data is used in aggregate and is not used to identify individual visitors.

13. Changes to this policy

We review this Privacy Policy at least annually and whenever our practices change. The current version and its effective date are shown above. Material changes will be published on our website.

14. Related documents

- Privacy Collection Notice
- Data Governance & Retention Policy
- Data Breach Response Plan
- Information Security Policy