

Information Security Policy

Dash Media Limited · Version 1.0 · Effective 27 October 2026 · Review by 27 October 2027 · Owner: Brad Hook, Director, Dash Media Limited

1. Purpose

This policy sets out how Dash Media Limited protects the information it holds on behalf of clients, participants, and itself. It is the parent document for the policies listed in section 8.

2. Scope

This policy applies to all products and services operated by Dash Media Limited, including:

- The FLAME app and program materials (flame.live)
- The Values Institute assessment and the Values Coach Certification (values.institute)
- Any future product operated by the company

It covers all systems, accounts, devices, and people with access to company or client information. At the date of this version, that is one person: the Director, who is also the sole developer and operator.

3. Principles

Minimum data. We collect only what a product needs to work, keep it only as long as it is useful, and delete it when it is not.

Certified infrastructure, small footprint. We build on providers that hold recognized certifications (SOC 2, ISO 27001) and keep our own layer simple enough to describe fully on a single public page.

Defense by default. Encryption, multi-factor authentication, row-level access rules, and automated backups are configured once and left on. We don't rely on remembering to be careful.

Honesty about limits. We are a small company. Where we lack a control that a larger organization would have, we say so rather than imply it.

4. Roles and responsibilities

The Director is accountable for information security, including:

- Approving and reviewing this policy and its sub-policies
- Managing all administrative access
- Selecting and reviewing subprocessors
- Responding to security incidents and data subject requests
- Keeping the public Trust Center accurate

If the company engages contractors or staff with access to client data, this policy and the Access Control and Acceptable Use Policy apply to them, and the Director records their access in the access register (see that policy).

5. Risk approach

Risk is assessed informally but on a schedule: at each annual policy review, and whenever a product adds a new category of data, a new subprocessor, or a new class of user. The assessment asks three questions: what could go wrong, how likely is it, and what would it cost the people whose data we hold. Controls are chosen in proportion to the answer.

The highest-rated risks at the date of this version are: compromise of the Director's administrative accounts; a bug that exposes one participant's data to another; and loss of availability of a subprocessor. The controls for each are described in the sub-policies.

6. Information classification

CLASS	EXAMPLES	HANDLING
Participant data	Names, email addresses, assessment responses, reports	Encrypted at rest and in transit; access limited by Row Level Security; retained per the Data Protection policy; never used for marketing
Client business data	Contracts, invoices, contact details of client staff	Stored in company email and accounting systems; not in product databases
Company confidential	Source code, credentials, financial records	Credentials in environment configuration only; source in private repositories
Public	Marketing content, published policies, program descriptions	No restriction

7. Compliance

Dash Media Limited is a New Zealand company and complies with the Privacy Act 2020. For clients and participants in other jurisdictions, we apply the same standards and will enter into a data processing agreement on request. We do not currently hold a SOC 2 report or ISO 27001 certification in our own name; our subprocessors do, and their reports are linked from the Trust Center.

8. Related policies

1. Access Control and Acceptable Use Policy
2. Data Protection, Retention and Deletion Policy
3. Secure Development and Change Management Policy
4. Incident Response Policy
5. Business Continuity and Disaster Recovery Policy
6. Vendor and Subprocessor Management Policy

9. Review

This policy is reviewed at least annually and after any security incident, major product change, or change in the people who have access. Each review is recorded with the date and a summary of changes.

10. Version history

VERSION	DATE	CHANGE
1.0	2026-10-27	Initial publication