

Access Control and Acceptable Use 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

To define who can access company and client information, how that access is granted and protected, and what acceptable use looks like.

2. Administrative access

Administrative access means any account that can read or change participant data outside the product's normal user interface, deploy code, or change infrastructure configuration. At this version, the systems with administrative access are:

SYSTEM	PURPOSE	ADMINISTRATORS
Vercel	Hosting, deployment, environment variables	Director
Supabase	Database, authentication, backups	Director
GitHub	Source code	Director
Google Workspace	Company email, documents	Director
Anthropic Console	API keys for the Claude API	Director
Namecheap (registrar) and Cloudflare (DNS)	Domains	Director

Rules:

- Multi-factor authentication is required on every administrative account, using an authenticator app or hardware key, not SMS where the provider allows a choice.
- Each person has their own account. There are no shared logins.
- Access is granted on a least-privilege basis. Contractors, if any, receive access to the specific project and role they need, for the duration they need it.
- The Director keeps an access register listing every person with administrative access, the systems, and the date granted. It is reviewed quarterly and when anyone's role changes.
- Access is removed on the same day a contractor's engagement ends.

3. Participant and client access

- Participants authenticate with a one-time code sent to their registered email address. The code is single-use and expires after 60 minutes. No passwords are created or stored.

- Participants can see only their own data. This is enforced in the database by Row Level Security, not only in the application code.
- Team administrators (a client's nominated person) can see who has joined their team and when they checked in, and a team report of averages once at least four people have checked in. They cannot see other teams, and they see an individual's responses only if that person has switched sharing on.
- Sessions last until the person signs out; the access token is renewed every hour. Signing out invalidates the session immediately.

4. Credentials and secrets

- API keys, database connection strings, and service tokens are stored in Vercel and Supabase environment configuration. They are never committed to source code, pasted into chat tools, or stored in documents.
- Keys are rotated when a person with access leaves, when a key may have been exposed, and otherwise at least annually.
- The Director uses a password manager for all account credentials.

5. Devices

- The Director's work device uses full-disk encryption, automatic operating-system updates, a screen lock, and a current browser.
- No participant data is stored on local devices except transiently during development against a local or staging database. Production database exports are not downloaded to local devices unless needed for a specific support task, and are deleted when the task is done.

6. Acceptable use

People with access to company systems must:

- Use access only for the purpose it was granted
- Not attempt to access another person's data, even if a bug makes it possible; report the bug instead
- Not share credentials, forward sign-in codes, or let others use their session
- Not install software or browser extensions on work devices that could read page content or credentials without a clear need
- Not use company systems to send unsolicited email or to process data for any purpose outside the published Privacy Policy

Participant data is never used for marketing, profiling for advertising, or sale to third parties.

7. Review

Reviewed annually and whenever administrative access changes.

8. Version history

VERSION	DATE	CHANGE
1.0	2026-10-27	Initial publication