Security summary

For IT, privacy and risk teams · Last updated 25 September 2026

Champ is a shared online space for the team around a child with extra support needs: parents, teachers, teacher aides, therapists and specialists. It is run by Champ Limited (NZBN 9429053962515), a small New Zealand company set up by two parents in Wellington.

This summary is for IT, privacy and risk teams deciding whether their staff can use Champ. It follows the headings of the New Zealand Information Security Manual (NZISM) so it can be compared with other systems. Champ has not been independently certified or tested against the NZISM or any other standard; this is our own account of how it works, and the last section says plainly what is not in place yet.

Questions go to our privacy officer, Jan-Paul de Groot, at hello@champ.kiwi.

1. Information Champ holds

About the adults who use it: name, email address, a scrambled (hashed) password, and optionally a photo, phone number, address and workplace.

About children, only what their team chooses to add: name, date of birth, school and class, photos, descriptions of what helps and what is hard, goals and progress, documents such as reports and plans, meeting notes, messages between team members and, where a parent switches that section on, medication details and a dose log. Much of this is health and disability information, which we treat as sensitive information under the Privacy Act 2020 and the Health Information Privacy Code 2020.

Children do not have accounts. A child's parents or guardians always manage their child's profile.

2. Where information is stored and processed

The database and uploaded files are held by Supabase in its Sydney, Australia region, on Amazon Web Services infrastructure.

The website and its server code run on Netlify, with the server code in Sydney, Australia.

A small number of other services process information for one purpose each: Resend sends Champ's emails; Deepgram turns meeting recordings into text; Anthropic's AI drafts plain-language summaries and meeting notes; Google Analytics counts visits to the public pages only, never a page about a child. Email to hello@champ.kiwi is forwarded by ImprovMX to a Google mailbox. Several of these companies are based in the United States.

Every provider stores and processes information only on our instructions and is contractually barred from using it for its own purposes, including training AI models. Sending information to Australia and the United States is a disclosure outside New Zealand under the Privacy Act; principle 12 of our Privacy Act statement explains why we are satisfied it is protected to a comparable standard.

3. Encryption

All traffic between a person's device and Champ is encrypted with TLS (HTTPS). Browsers are told to use HTTPS only (HTTP Strict Transport Security).

Supabase encrypts the database, uploaded files and backups at rest with AES-256.

Passwords are stored only as a salted hash by Supabase's sign-in system; nobody, including us, can read them.

Files are never public. Opening a document gives the browser a private link that expires after two minutes, and only after the database has confirmed the person may see it.

4. Access control

Every child has a team. The people who manage a profile (normally the parents) invite each member and give them one of three levels: manages everything, can add and update, or can see everything. They can also limit a person to particular parts of the profile or particular documents. The medication section is switched off for everyone until a manager turns it on for the people who need it.

These rules are enforced inside the database with row-level security on every table, not only on the screen. A person cannot reach a profile they are not on, even by calling the database directly.

A school or practice supervisor can see which children their staff work with, but must join a child's team, visibly, to open the profile, and the parents are told. The same rule applies to the two people who run Champ: we open a profile only when a family asks us to help, by joining the team visibly, and leave when done.

Everyone with access is listed on the child's Team page. There are no hidden viewers.

5. Signing in

Accounts are by invitation only; open sign-up is switched off. People sign in with an email address and a password of at least 8 characters, or with a one-time link sent to their email.

Two-step sign-in is available to everyone: once switched on in Settings, signing in also needs a 6-digit code from an authenticator app. It is required for the two people who run Champ. The database itself refuses any session for that person that has not passed the code, so the check cannot be skipped by going around the website.

Each person gets 10 single-use backup codes for a lost phone, stored only as a fingerprint (hash). Using one switches two-step sign-in off, signs the account out everywhere and emails the person. If someone has lost both, we switch it off only after confirming who they are, and email them when we do.

Changing a password signs the account out on every other device. Unused accounts can be identified and closed.

6. Administration of the systems behind Champ

Only the two people who run Champ can reach the hosting, database and email accounts, each protected with two-step sign-in.

Service keys and passwords live in the hosting provider's protected settings, never in the code. The build process scans for secrets accidentally included in the code and stops if it finds one.

7. Logging and monitoring

Each child's profile keeps an activity history of what was added or changed and by whom, visible to the people who manage it. Managers are notified when someone joins the team, adds something or records a meeting.

Supabase and Netlify keep their own logs of sign-ins, database activity and requests, which we can review if something looks wrong. Champ does not have round-the-clock security monitoring.

8. Backups and recovery

Supabase backs up the database automatically every day and keeps each backup for 7 days. Uploaded files are held on Supabase's redundant storage; they are not part of the daily database backup.

The people who manage a profile can download everything in it, documents included, at any time from the profile's About page.

9. Keeping and deleting information

A profile stays as long as its team wants it, because continuity across years and schools is the point of Champ. Its managers can delete it at any time; it is removed straight away, apart from backups, which roll off within the backup period.

Meeting audio is deleted as soon as it has been turned into text, usually within minutes. Demo accounts, which contain only a fictional child, are deleted after 14 days. Requests for access are deleted once the person has joined, or after 90 days.

A person can close their own account at any time. If Champ ever closes, every profile's managers get at least 90 days' notice and a way to download everything, after which all data, files and backups are deleted.

10. Artificial intelligence

AI is used for three things only: plain-language summaries of documents, draft notes from meeting transcripts and, when a parent asks, a first draft of the About sections. Nothing an AI writes is shown to the team until a person has checked and approved it.

Text and audio are sent to Anthropic and Deepgram only to produce that result, and neither uses it to train its models. Every request to Deepgram opts out of its model improvement programme, so audio is kept only as long as the transcription takes. Anthropic deletes text from its systems within 30 days under its commercial terms (longer only if it were flagged as breaking Anthropic's usage rules). Champ never uses information to train anything, and never sells it or uses it for advertising.

11. Incidents and privacy breaches

We have a written breach response plan. If we become aware of a privacy breach that has caused, or is likely to cause, serious harm, we notify the Office of the Privacy Commissioner and the people affected as soon as practicable, as Part 6 of the Privacy Act requires, and tell them plainly what happened and what we are doing about it.

Organisations whose staff use Champ can ask to be told directly of any incident affecting their people.

12. Building and changing Champ

Champ is built by the two people who run it, using well-supported open-source frameworks and managed services rather than self-run servers, so operating-system and database patching is done by the providers.

Each change is built and checked before it goes live, including automated accessibility checks. Standard protective web headers are sent on every page.

13. What is not in place yet

We would rather say this than have it found. Champ has not had an independent penetration test or a certification such as ISO 27001 or SOC 2. There is no round-the-clock monitoring. Two-step sign-in is optional for everyone except the people who run Champ. Champ is run by two people, which keeps access tight but means a small team.

If your organisation needs more before its staff use Champ, tell us what. We are happy to answer a security questionnaire, talk to your IT team, and consider an independent test with an organisation that plans to adopt Champ.