Trust

Security & data handling

Last updated 12 November 2026 · Operator: Daniel Gosling, trading as GearQ · Melbourne, Victoria, Australia · Security contact: hello@gearq.app

This page explains, in plain terms, how GearQ protects your group's gear records and the small amount of personal information it holds. It's written so a quartermaster, a group leader, a district commissioner or an IT volunteer can all check it for themselves. Every technical number on this page is taken from GearQ's code, and an automated check stops a release if the code and this page disagree.

The short version

GearQ is gear management, nothing else. About the people who book gear it keeps only their *name, email and phone number*, so the quartermaster can contact them about that booking, and it anonymises them 12 months after the booking ends. (Quartermasters and helpers with their own login have a name and email on file.) No medical details, no children's details, no dates of birth, addresses or member numbers, no connection to any Scouts system. Your gear list is never public. Everything runs on Cloudflare, encrypted in transit and at rest, with a nightly backup that we have restored and checked. Automatic security monitoring checks GearQ every 15 minutes and alerts GearQ's operator — never anyone else. No advertising, no tracking. We're honest below about what we don't do yet.

On this page

1. What we store, and never store
2. Your gear stays private
3. Hosting & data residency
4. Encryption
5. Passwords & sign-in
6. Group isolation
7. No connection to Scouts systems
8. Sub-processors
9. Backups & restore
10. Monitoring & breach response
11. Export, deletion & retention
12. Child safety
13. Honest gaps
14. Report an issue

1 What we store, and never store

We can't lose what we never collect.

Data	Stored?	Where / who sees it
Name, email and phone of the person booking gear	**Yes**	GearQ database. Email and phone: only your group's quartermaster(s) and helpers, the booker (via their own link), and GearQ's operator for support. The booker's name and section also show on your group's own booking calendar, to people with your member password. Never districts or regions. Anonymised 12 months after the booking ends.
Name and email of quartermasters and helpers you invite	**Yes**	GearQ database, so they can sign in.
Name, email and phone of an adult asking an activity team for support	**Yes**	GearQ database. Seen only by that team's quartermasters, the branch's named admin and GearQ's operator for support. The requester's status link shows the request and reply, never contact details; it is stored only as a hash and expires 30 days after the event. Branch viewers see counts only. Youth and leaders are recorded as numbers, never names. Anonymised 12 months after the event.
Gear: items, quantities, serial numbers, storage notes, maintenance notes, photos of gear	**Yes**	GearQ database, behind your group's passwords.
Network (IP) address and country, in the security log	**Yes, 90 days**	Every sign-in (successful or not, for every kind of login), refused requests, exports, password resets and logo uploads are logged with the network address and the country Cloudflare reports. Used only to detect misuse; only GearQ's operator sees it. The address and country are deleted after 90 days (failed-sign-in counters after about a day). The activity log of who changed what, and a group's sign-up record, also hold an address — those don't expire yet (see Honest gaps).
Passwords	Only as a salted hash	Never stored or logged as plain text.
Stripe customer and subscription reference	**Yes**	A reference only; the billing record lives at Stripe.
Card numbers	**No**	Entered directly into Stripe; never reaches GearQ.

Data	Stored?	Where / who sees it
Medical details, allergies, dietary needs	**Never**	—
Children's details (names, ages, photos, sections)	**Never**	—
Dates of birth, home addresses, member or registration numbers	**Never**	The database has no field for any of these, and a release check fails if one is added.
Advertising or tracking data	**Never**	No analytics, advertising or tracking scripts. Fonts are served from gearq.app.

Free-text notes are for gear. Every booking form says *"Gear notes only — please don't include medical, personal or contact details"*, and the quartermaster's view flags notes that look like they contain an email address, a phone number or medical details so they can be edited out. GearQ flags; it never silently changes what someone wrote.

2 Your gear stays private

A list of what a group owns and where it's kept is a shopping list for a thief. So:

- Your gear list, storage locations, serial numbers, photos and bookings are **never public**. They are only shown after signing in with your group's password.
- Group, district, region and owner pages tell search engines not to index them (a `noindex` header and tag, plus `robots.txt`). The public website only ever shows made-up example gear.
- A district or region sees **counts only** (for example "3 canoes"), never locations, serial numbers, notes, photos or who booked — and only if your group chooses to share. The default is private.

3 Hosting & data residency

GearQ runs entirely on Cloudflare: Cloudflare Pages and Workers run the app, Cloudflare D1 is the database, Workers KV holds the backups, and Cloudflare Email Service sends email. GearQ has its own Cloudflare account and its own Stripe account, separate from any other business.

The database runs in Cloudflare's **Asia-Pacific (APAC)** region. That is **not guaranteed to be inside Australia**, and pages are served from Cloudflare's worldwide network (for Australian users, usually an Australian data centre). Cloudflare holds SOC 2 Type II and ISO/IEC 27001

attestations, among others — see Cloudflare's compliance resources (gearq.app/security). Those are Cloudflare's certifications, not GearQ's.

4 Encryption

- **In transit:** every page and API call is HTTPS (TLS). Plain HTTP is redirected to HTTPS, and browsers are told to insist on HTTPS for a year (`Strict-Transport-Security: max-age=31536000`).
- **At rest:** Cloudflare encrypts stored data, including the database and backups.
- **Browser hardening:** every response sets `X-Content-Type-Options: nosniff`, a `Referrer-Policy`, framing limits (`X-Frame-Options`), and a `Permissions-Policy` that switches off camera, microphone, location, payment and USB access.
- **Payments:** handled entirely by Stripe. GearQ never sees a card number.

5 Passwords & sign-in

- **Passwords are hashed** with PBKDF2-SHA256, 100,000 iterations, a random 16-byte salt per password, compared in constant time. A missing or damaged hash never matches anything.
- **Each group has two shared passwords**: one for members (to book) and one for the quartermaster. Passwords must be at least 8 characters; sign-up also refuses common passwords and requires the two to differ.
- **Guessing is limited:** 10 wrong tries per network address, per group and password, in 15 minutes, and then that address must wait. The owner's backup password allows 5 wrong tries per 15 minutes.
- **Sessions** are random 256-bit tokens recorded on the server, so they can be ended at any time (the owner can sign everyone out of a group). The quartermaster's session ends after 2 hours without use; a member's lasts 30 days.
- **Named logins:** quartermasters and helpers can have their own login by emailed one-time link (an invitation works once within 7 days; a sign-in link works once within 15 minutes), so every change shows who made it. Helpers can be view-only.
- **The GearQ owner** signs in with a one-time link that works once within 15 minutes and is only ever sent to one fixed address, or with a backup password of at least 10 characters. The owner can look at a group only through a read-only, single-use link that expires after 5 minutes, and every owner action is written to an audit log.

6 Group isolation

Every request is tied to exactly one group, and every database query is filtered by that group. A sign-in for one group is refused by every other group, and signed links in emails carry the group inside the signature, so a link for one group can never act on another. Districts and regions have their own sign-ins that can read counts only (and, for groups that allow borrowing, send a borrow request into that group's queue for its quartermaster to approve). They can never see or change a group's gear list or bookings.

This is checked by automated tests on every release cycle, against the live system: in the latest full run (12 November 2026) 370 live checks across six suites and 67 offline unit tests all passed — among them 29 unit tests of the access rules, 13 tenant-isolation checks that try to use one group's sign-in, links and lockouts against another group, and 128 district/region checks. They include tenant isolation, cross-group link refusal, district/region access rules, and scans proving roll-ups never contain serials, locations, notes or booker details.

7 No connection to Scouts systems

GearQ is independent software. It is not affiliated with or endorsed by Scouts Australia or any Scouts branch. It has no connection to Scouts membership systems (such as the Extranet or Operoo) and never imports anyone's personal details on a group's behalf. The spreadsheet import only accepts gear (item, category, quantity, serials, notes) and cannot create people or bookings. A release check fails if GearQ's code ever references those systems.

8 Sub-processors

Provider	What for	What it sees
Cloudflare, Inc.	Hosting, database, backups, email sending, the spreadsheet-reading library (cdnjs, loaded only when a quartermaster imports an Excel file)	Everything GearQ stores
Stripe	Subscription billing and payments	The paying group's billing contact and payment method

We don't sell data and don't disclose it for advertising. If we add a provider that processes customer data, we'll update this list and tell groups before it's used.

9 Backups & restore

- Every night a scheduled job copies the whole database (except live sign-in sessions) to a private backup store in GearQ's own Cloudflare account. We keep the last 30 daily copies and one copy per month for 12 months.
- Cloudflare D1 also keeps its own point-in-time history ("Time Travel"), which can roll the database back to any minute in the last 30 days.
- **Restore tested:** on 11 November 2026 a real backup was restored into a separate, temporary database and every table was compared with the backup — 29 tables, 996 rows, all identical — then the temporary database was deleted.

10 Monitoring & breach response

Automatic monitoring. A scheduled check runs every 15 minutes. It looks for:

- **Gear visible without signing in** — it asks every group's booking page, quartermaster screens, exports and the district, region and owner views for data *without* a sign-in, and treats any answer with data as critical. Each run also makes one request that *must* see data (a short-lived sign-in to made-up demo data), so a broken check can't quietly report "all clear".
- **Password guessing** — bursts of wrong passwords against one group or from one network address, lockouts, and failed owner sign-ins.
- **The owner account** signing in from a new network address or country.
- **Snooping** — a signed-in person repeatedly asking for another group's or store's data.
- **Unusual downloads** — far more exports than a group normally makes, or an export soon after a sign-in from a new address.
- **Data disappearing** — a group's gear or bookings dropping sharply without matching deletions in its activity log.
- **Safety settings and health** — the security headers on this site, this page being up, and the nightly backup and retention jobs having run.

Alerts go to GearQ's operator only — by email and by a private message — and repeat until the operator acknowledges them. Groups are never emailed automatically by the monitoring. An alert is a sign to investigate, not proof of a breach.

If it is a breach. GearQ follows the Notifiable Data Breaches scheme under the *Privacy Act 1988* (Cth). We contain it first, then assess it promptly (and within the 30 days the law allows). Once we have **confirmed** a breach that touches a group's data, we tell that group's quartermaster within 72 hours, by email written and sent by the operator (what we know, what we're doing, what you can do). If it is likely to cause serious harm, we also notify the Office of the Australian Information Commissioner (OAIC) and the people affected.

11 Export, deletion & retention

- **Export:** a quartermaster can download the group's whole gear list as a spreadsheet at any time, even if the plan has lapsed.
- **Correction and deletion:** a quartermaster can edit or remove booking details directly, and anyone can ask us to see, correct or delete their details at hello@gearq.app. A group can ask us to delete the whole group.
- **Automatic anonymising:** a daily job removes the name, email and phone of the person booking 12 months after a booking ends (the gear history stays, without the person). Copies of emails GearQ sent are deleted after 12 months, and failed sign-in records after about a day.
- **Lapsed groups:** nothing is deleted because a plan lapsed. After 2 years with no active plan, a group's data is deleted, with a warning email to the quartermaster at least 30 days beforehand.
- Deleted data ages out of the backups within 30 days (daily copies) and 12 months (monthly copies).

12 Child safety

GearQ is a gear tool for adults: leaders, quartermasters and parents. It does not ask for or hold any information about children — no names, ages, photos, health or behaviour. People making bookings must be 18 or over. There's no advertising, no profiling and no use of anyone's data to train AI.

13 Honest gaps

- **GearQ is not SOC 2 or ISO 27001 certified.** It runs on Cloudflare, which is; GearQ itself has a written readiness plan, not a certificate.
- **One operator.** GearQ is run by one person, so there is no second person reviewing every change.
- **No independent penetration test yet.**
- **Data region is Asia-Pacific, not guaranteed Australia.**
- **The terms and privacy policy are drafts awaiting a lawyer's review.**
- **Shared group passwords** are convenient but anyone who has the member password can book. Change it if it leaks; named logins exist for quartermasters and helpers.
- **Password hashing** uses 100,000 PBKDF2 iterations — the most Cloudflare Workers allows — which is below the 600,000 that OWASP currently recommends for PBKDF2-SHA256.
- **No two-factor sign-in** for quartermasters yet (named logins use emailed one-time links, which rely on the security of your email).
- **Backups live with the same provider** (in GearQ's own Cloudflare account), not a second company.
- **Monitoring has limits.** It looks at GearQ's own logs and answers every 15 minutes; it can't see someone using a correctly guessed or shared password who behaves normally, problems at Cloudflare itself, or anything in the gap between checks. One person receives the alerts, so a response overnight may take hours.
- **Some network addresses don't expire yet:** the security log's addresses are deleted after 90 days, but the per-group activity log and a group's sign-up record still keep theirs.

14 Report an issue

Found a security problem, or worried about your data? Use the form below (at gearq.app/security#report), or email hello@gearq.app with "Security" in the subject. Please don't test against other groups' data. We'll acknowledge within 3 business days.

See also: Privacy policy · Terms

© 2026 GearQ · GearQ is independent software. It is not affiliated with or endorsed by Scouts Australia or any Scouts branch.