

Data Exposure Report — Squadi / NetballConnect Platform

Date: 23 February 2026 (updated 24 February 2026) **Reporter:** Casey Toll — Parent and coach at Hazel Glen Netball Club **Severity:** Critical — Children's personal information openly accessible online

What Happened?

The registration system used by netball clubs across Australia — **NetballConnect**, built by a company called **Squadi (World Sport Action)** — has a serious security flaw. The personal details of every registered player are accessible to anyone on the internet. **No login, no password, and no special tools are required.**

The information exposed includes:

- **Children's full names**
- **Children's dates of birth**
- **Parent/guardian email addresses**
- **Parent/guardian phone numbers**
- **Which team and competition they play in**

This is not a theoretical risk. I was able to look up my own daughter's full details — her name, date of birth, my email address, and my phone number — in a matter of seconds. 2

How Was This Discovered?

I'm a parent and coach at Hazel Glen Netball Club. In my own time, I've been building a personal team management app to help with coaching duties. As part of that hobby project, I was looking at how to pull in publicly available ladder and fixture data from the Squadi system.

During that work, I discovered that the NetballConnect website contains a **secret access key embedded in its publicly visible code** — the equivalent of publishing a password on the front page of a website. Using this key, I found that anyone can retrieve the full personal details of every registered player on the platform.

I was not looking for this vulnerability. I discovered it by accident. The app I'm building is an unofficial personal project — it is not endorsed by or affiliated with Hazel Glen Netball Club, Nillumbik Force, or Netball Victoria.

How Easy Is It to Access This Data?

Extremely easy. To put it in non-technical terms:

1. **Visit the NetballConnect website** — the access key is sent to your browser automatically
2. **View the page source** — something any browser can do (right-click → View Source)
3. **Copy the access key** — it's clearly labelled in the code
4. **Use it to request player details** — paste a web address into your browser with the key

A curious teenager could do this. No hacking knowledge, no special software, no criminal tools. Just a web browser.

There is also nothing stopping someone from writing a simple program to **automatically download every player record on the platform in a matter of hours**. There are no limits on how many requests can be made or how fast.

How Many People Are Affected?

Confirmed

I verified the exposure against my own club (Hazel Glen Netball Club) in the 2026 NFNA Saturday Autumn competition:

- **10 Hazel Glen teams checked** — all 90 players' personal details were accessible
- **100 teams total in the NF competition** — approximately 900 players exposed in this one local competition alone
- **My daughter's full record was returned** — name, date of birth (she is 13), my email, my phone number

Estimated National Scale

- The platform contains **over 1.27 million player registration records** for netball alone
- Competition records go back to **at least 2022** — old data is still accessible
- **Conservative estimate: 300,000 to 500,000 children's records are exposed** (many players re-register each season, so there are duplicate records, but historical data including old contact details remains accessible)

It's Not Just Netball

I also confirmed that the **same access key works on two other Squadi sports platforms**:

- **Basketball** (`api-basketball.squadi.com`) — player PII confirmed exposed
- **Football/Soccer** (`api.squadi.com`) — player PII confirmed exposed, using a different server but the same access key

Squadi's three main sports platforms — netball, basketball, and football — are all affected. The total number of affected individuals across all sports could exceed **one million**.

How Long Has This Been Going On?

Using the Internet Archive (a public service that takes snapshots of websites over time), I checked historical versions of the NetballConnect website:

- **The earliest snapshot available is from November 2023**
- **The access key was already present in December 2023** — over 2 years ago
- **The same key has been present in every version of the website since then** — it has never been changed
- Player data from competitions labelled "2022" is still accessible

This data has been exposed for at least 2 years, possibly longer. During that time, the key has never been changed, which suggests the company has no process for monitoring or rotating access credentials.

There is no way to know if someone else has already downloaded this data. Only Squadi can check their systems to determine if any bulk data extraction has occurred.

What Could Someone Do With This Data?

The combination of information available creates serious risks:

- **Contact children's families directly** — an attacker knows the child's name, age, which team they play for, where they play (venue addresses are also public), and has the parent's email and phone number
- **Send convincing fake messages** — for example: *"Hi [parent name], this is regarding [child name]'s registration for [competition name] at [venue]. Please click here to update your details."* Every detail needed to make this message believable is available through the platform
- **Download the entire national database** — with no limits on access speed, a simple automated script could extract every record on the platform in hours
- **Identity-related fraud** — children's dates of birth combined with parent names and contact details provide a foundation for identity fraud, which is particularly concerning for minors whose credit histories are rarely monitored

Why This Matters Legally

Under Australian law, organisations that handle personal information have specific obligations:

- **The Privacy Act 1988** requires organisations to take reasonable steps to protect personal information from unauthorised access. Publishing an access key in publicly visible code does not meet this standard.
- **The Notifiable Data Breaches (NDB) scheme** requires organisations to notify the **Office of the Australian Information Commissioner (OAIC)** and all affected individuals when a data breach is likely to result in serious harm. Children's personal details being openly accessible for 2+ years almost certainly meets this threshold.
- **Children's data receives heightened protection** under Australian privacy law. The majority of records in this system belong to minors.
- **Both Squadi and the sporting organisations** (such as Netball Victoria and its affiliated associations) may share responsibility — Squadi built and operates the platform, but the sporting bodies collected the data through it.

Once an organisation becomes aware of a potential breach, a 30-day assessment period begins under the NDB scheme. This report constitutes notification.

What Needs to Happen

Immediately

1. Squadi must **remove the published access key** from their website code
2. Squadi must **restrict access to player personal details** so that only authorised people (coaches, administrators) can see them, and only for their own teams
3. Squadi must **check their system logs** to determine whether anyone has already bulk-downloaded player data

Within Weeks

4. Squadi must **review all parts of the system** that return personal details and ensure proper access controls are in place
5. The **NDB notification obligations** must be assessed — if the breach meets the serious harm threshold, Squadi and the sporting bodies must notify the OAIC and affected individuals
6. **All access keys must be changed** — the current key has been publicly available (including in internet archives) for over 2 years and must be considered compromised

Within Months

7. A **full security review** of the platform should be conducted across all sports
8. A **proper access control system** should be implemented that separates public information (ladders, scores, schedules) from private information (player details, contact information)

Who Needs to Be Informed?

Organisation	Why
Squadi / World Sport Action	They built and operate the platform — they must fix the problem
Netball Victoria	They are responsible for the data of Victorian netball players collected through this platform
Netball Australia	The exposure is national — all states and territories are potentially affected
Basketball bodies	The basketball platform is confirmed to have the same vulnerability
Football Australia / state bodies	The football/soccer platform is confirmed to have the same vulnerability
OAIC	The privacy regulator — must be notified if Squadi doesn't act, or if NDB obligations are triggered

Suggested Netball Victoria Contacts

- **Penny Forrest** — Child Safety & Integrity Coordinator
- **Rebecca Costanzo** — Head of Integrity and Compliance
- **Rohan Safstrom** — IT Support and Services Manager
- **Ginny Robinson** — Systems Relationship Manager

About This Report

This report is provided in good faith as a **responsible disclosure**. I discovered this issue by accident while working on an unofficial personal project. I have not extracted any data beyond what was needed to verify the problem, and I have not shared the access key or any player data with anyone.

I verified the vulnerability using my own daughter's registration record, with my consent as her parent.

A **separate technical report** with full details of the specific systems, endpoints, and code involved is available for Squadi's engineering team.

I am willing to assist with any questions about the findings or the remediation process.

Casey Toll Parent and Coach — Hazel Glen Netball Club 23 February 2026

This report represents my own findings as an individual. It is not made on behalf of Hazel Glen Netball Club, Nillumbik Force Netball Association, or any other organisation.