Privacy Policy

Website and client portal

Safer Centres

Document	Privacy Policy
Version	1.3
Owner	Joy Mulquiney, Privacy Officer
Approved by	Directors
Effective date	5 November 2026
Last reviewed	5 November 2026
Next review	5 November 2027
Applies to	Website and client portal

Safer Centres helps organisations such as childcare centres, early learning centres and churches create safer environments for children. This policy explains how we collect, hold, use and share personal information through our website (www.safercentres.com.au) and our client portal. We handle personal information in line with the Privacy Act 1988 (Cth) and the Australian Privacy Principles, the Health Records and Information Privacy Act 2002 (NSW) where it applies, and, for anyone it covers, the EU and UK General Data Protection Regulation (GDPR).

1. Who we are

Safer Centres Pty Ltd (ABN 37 703 044 286) ("Safer Centres", "we", "us"). Our Privacy Officer is Joy Mulquiney, reachable at info@safercentres.com.au or Suite 17, 89-97 Jones Street, Ultimo NSW 2007.

2. What we collect

Who	What we collect
Website visitors	Device and browser details, IP address, pages visited and cookies. Anything you put in an enquiry, lead or waitlist form: name, email, phone, organisation, role, location and message.
Client contacts (directors, leaders, administrators)	Name, role, work contact details, portal login details (passwords are stored in encrypted form), messages to us, meeting and reminder details, and invoicing contact details.
Staff and volunteers of our clients	Names, dates of birth, email addresses, roles, teams and information provided in the compliance dashboard, such as Working With Children Check numbers, issue and expiry dates, first aid and CPR certificates, police check dates, training records and copies of certificates, supplied by the client.
Child safety records	Assessment and audit findings, policies and other documents clients add to the portal. These can include children's names or ages and health, medical or allergy details. We ask clients to leave out identifying details about children unless they are needed.

People who use our Tell Us inbox	What you tell us in the form, including details about named people, and your name and contact details if you choose to give them. You may stay anonymous.
Portal users	Login times, activity logs and the documents and messages you upload or send.

Some of this is sensitive information, including health information, religious information, criminal records and allegations about individuals. We collect sensitive information only with consent, or where the law allows or requires it.

3. How we collect it

We collect information directly from you, from our clients (who are often the original source), automatically through our website and portal, and through our Tell Us inbox. We may also use information that is publicly available where it is needed for our services. You can deal with us anonymously or under a pseudonym where that is practical, for example when browsing our website or using our Tell Us inbox. We cannot deliver most client services this way.

4. Why we use it

Purpose	GDPR lawful basis (where GDPR applies)
Respond to enquiries and manage the waitlist	Consent or steps before a contract
Deliver our services: assessments, reports, audits, workshops, dashboard and portal	Contract
Track compliance expiry dates and send reminders, including, where a client turns this on, emailing its staff and volunteers before their Working With Children Check expires	Contract and legitimate interests
Receive child safety concerns and pass them to the relevant centre	Legitimate interests (protecting children), plus consent or legal obligation for sensitive information
Invoicing, accounting and record keeping	Contract and legal obligation
Keep our systems secure and improve our website	Legitimate interests
Send updates about our services	Consent (you can withdraw it at any time)
Meet our legal obligations	Legal obligation

Use of artificial intelligence (AI). We use AI platforms to help our team work efficiently, for example to draft, summarise or check documents such as reports, policies and correspondence. We use business versions of these platforms that do not use our information to train their AI models. We limit the personal information we put into them, and we do not put in information that identifies children or people named in a concern. A member of our team reviews anything AI helps to produce before it is used or shared, and we do not use AI to make decisions about individuals. Our client portal does not send your information to AI platforms. Where an AI platform stores or processes information overseas, section 12 applies.

5. Who we share it with

- **The relevant centre.** Concerns raised through our Tell Us inbox are passed to the centre's Director or, if the concern is about the Director, to the body the centre nominated when it joined us (such as its board, governing body or approved provider), as that centre's independent safety partner.
- **Our service providers.** These include hosting, email, file storage, scheduling and accounting providers, listed in section 12. They may use information only to provide services to us and must keep it confidential.
- **Professional advisers**, such as lawyers, accountants and insurers.

- **Authorities and other parties** where the law requires or authorises it, or where we reasonably believe sharing is needed to prevent a serious threat to a child's safety.
- **A buyer or successor** if our business is restructured or sold, subject to confidentiality.

We never share client information with other clients.

6. Tell Us inbox

People connected to a centre we work with, such as parents, carers, staff and volunteers, can raise a child safety concern with us through our Tell Us inbox, by scanning the QR code displayed at the centre and filling in a short form. If you leave your contact details, we contact you within 24 hours.

- **What we do with your message.** We make a file note of what you tell us, then contact the centre's Director about the concern so the centre can take action. If the concern is about the centre's Director, we contact the body the centre nominated when it joined us (such as its board, governing body or approved provider) instead.
- **Mandatory reporting.** Each centre remains responsible for its own mandatory reporting to statutory authorities. We may also report a concern to police, child protection or other external bodies ourselves, where we consider it appropriate or where the law requires it, and we may need to disclose the information you give us, including your name and any names you provide.
- **Emergencies.** The Tell Us inbox is not monitored in real time. If a child is at immediate risk, call 000.
- **Anonymity and confidentiality.** You can stay anonymous, however this may limit the centre's ability to respond to the concern. If you give your name, we keep it confidential and share it only with your consent, or where we report a concern as described above.
- **Accuracy.** Our records reflect what the person told us. We do not investigate concerns or make findings about any person.
- **People named in a concern.** You can ask for access to information we hold about you. We may refuse or limit access where it would unreasonably affect another person's privacy, prejudice an investigation or put a child's safety at risk, and we will tell you why.
- **Records.** We keep what you submit and our file note for the periods in section 10.

7. Children's information and our role with client data

We do not collect information directly from children, and our website is not directed at children. Information about children reaches us only through our clients and our Tell Us inbox, and we use it only to deliver our services.

For information about a client's staff, volunteers and children held in the portal, the client decides what is collected and why. We handle it on the client's behalf under our service agreement and follow their lawful instructions. Clients are responsible for having authority to share this information and for giving their own staff and volunteers a notice about it. Within a client's portal, the client's Director decides who has access, and Key Leaders see only the people in the teams they lead. Where a client turns on reminder emails, we send them on the client's behalf to the email address the client has recorded. If you want to access or correct this information, we may refer your request to the client.

The portal is a workspace for the advice, reports and policies we deliver, not a filing system. Clients should keep their own original records. Clients can export their documents from the portal at any time and when our agreement ends, and we only ask clients to upload copies of records that we need to deliver our services. Clients keep their incident reports in their own systems, not in the portal.

8. Cookies and marketing

Cookies are small files a website saves on your device. We currently use only essential cookies, which keep our website and client portal working.

Type	What it does	Examples	Your choice
Essential	Keeps you logged in to the client portal, protects against fraud and remembers your cookie choices	Session and security cookies	Always on. The portal cannot work without them.

We do not use analytics or marketing cookies. If that changes, we will ask for your consent first and update this policy. You can block or delete cookies in your browser settings, though the portal may not work properly if you block essential cookies.

We send updates about our services only if you have asked for them or agreed to receive them, and every message has an unsubscribe link.

9. Security and data breaches

We protect personal information with encryption in transit and at rest, role-based access so each client sees only its own organisation's data (and, within a client, each person sees only what their role allows), multi-factor authentication for our staff and each client's Director, and regular access reviews. We keep Tell Us inbox records on access-restricted systems.

If a data breach is likely to cause serious harm, we will notify affected people and the Office of the Australian Information Commissioner (OAIC) as the Notifiable Data Breaches scheme requires. Where GDPR applies, we notify the relevant supervisory authority within 72 hours of becoming aware, where required.

10. How long we keep information

Information	How long
Our service data: assessments, reports, audit findings, recommendations and messages with clients	7 years from the end of the client relationship or the date of the record, then securely destroyed or de-identified
Tell Us inbox submissions and file notes	7 years from the date of the record, then securely destroyed or de-identified
Copies of client records that a client gives us (such as policies, library documents and staff or volunteer records, including copies of certificates)	Until the services end, then exported by the client or deleted or de-identified within 30 days of the agreement ending, unless we must keep them for legal reasons
Website enquiries and leads	2 years after our last contact with you
Waitlist and marketing list	Until you unsubscribe or ask us to remove you
Portal logs and security records	12 months

We keep our service data for the periods above because it may be needed for legal claims, regulator inquiries and reportable conduct matters. This can limit deletion requests during those periods. Where we keep a record involving alleged harm to a child for longer, we review it each year and destroy or de-identify it as soon as it is no longer needed. Our clients are responsible for keeping their own records for as long as the law requires them to, such as incident and injury records. The client portal is not a records system, and clients should keep their own original copies.

11. Your rights

Under Australian law, you can ask to access the personal information we hold about you and to correct it if it is inaccurate, out of date or misleading. We will respond within 30 days.

Under GDPR, where it applies, you also have the right to:

- erasure of your information, where we no longer need it or have no legal basis to keep it
- restriction of how we use it
- receive a copy in a portable format

- object to uses based on legitimate interests, and to direct marketing
- withdraw consent at any time, without affecting earlier use

To use any of these rights, email info@safercentres.com.au. We may need to verify your identity first. We may decline a request where the law allows or requires, for example where the record is needed for legal claims or to protect a child. We will explain our reasons in writing.

12. Service providers and overseas storage

We use trusted service providers to host, store and process information. Our client portal data is held in Australia. Some other information is stored or processed overseas, including in the United States, Europe and Japan, as set out below.

Type of provider	What for	Where information is held
Portal database and file storage	Client portal, documents, messages and backups	Australia
Email delivery	Portal notifications and reminder emails, including reminders to clients' staff and volunteers	Overseas, including Japan and the United States
AI platforms	Helping our team draft, summarise and check documents	Overseas, including the United States
Email, calendar and document storage	Day-to-day communication and working documents	Australia and overseas, including the United States and Europe
Website hosting and domain services	Our website and domain name	Australia and overseas, including the United States
Accounting and invoicing software	Invoicing and financial records	Overseas, including the United States

Before sending information overseas we take reasonable steps to make sure the recipient protects it in line with the Australian Privacy Principles, usually through contract terms. Where GDPR applies, we rely on an adequacy decision or standard contractual clauses for transfers.

13. Complaints

If you think we have breached your privacy, contact our Privacy Officer at info@safercentres.com.au. We will acknowledge your complaint within 5 business days and aim to resolve it within 30 days. If you are not satisfied, you can contact:

- the Office of the Australian Information Commissioner at oaic.gov.au
- the Information and Privacy Commission NSW at ipc.nsw.gov.au, for health information
- if GDPR applies to you, your local data protection authority

14. Changes to this policy

We may update this policy from time to time. The current version is always on our website with its last-updated date. We will tell portal users about significant changes.

15. Contact us

Joy Mulquiney, Privacy Officer, Safer Centres Pty Ltd (ABN 37 703 044 286)

Email: info@safercentres.com.au

Post: Suite 17, 89-97 Jones Street, Ultimo NSW 2007