
Brightside Connect Privacy Policy

Last updated: May 2026

This Privacy Policy explains how Brightside AI handles personal information in connection with Brightside Connect, including our website, software platform, mobile application, integrations, automation tools, artificial intelligence features, support services and related services.

By accessing or using Brightside Connect, creating an account, using our Services, submitting information to us, or authorising your organisation to use Brightside Connect, you acknowledge that we will handle personal information in accordance with this Privacy Policy.

This Privacy Policy should be read together with the Brightside Connect Terms and Conditions and any applicable subscription terms, order form, proposal, invoice, data processing terms or other written agreement between you and us.

1. About us

Brightside Connect is provided by Brightside AI.

Business name: Brightside AI

Trading name: Brightside AI

ABN: 13 461 862 094

Email: admin@brightsideai.com.au

Website: <https://brightsideai.com.au/>

In this Privacy Policy, Brightside Connect, Platform, Software, we, us or our means the Brightside Connect software, website, mobile application, tools, modules, integrations and related services provided by Brightside AI.

2. Application of this Privacy Policy

This Privacy Policy applies to personal information we collect, hold, use and disclose when providing Brightside Connect and related services.

Brightside Connect is designed for providers, organisations and care-based businesses. The Platform may be used to manage staff, support workers, participants, clients, representatives, emergency contacts, rostering, incidents, compliance, invoicing, documents, communications and related operational records.

Where a customer organisation enters information into Brightside Connect about its own participants, clients, staff, workers, contractors, representatives or other individuals, that customer remains responsible for ensuring that it has the right to collect, use, upload, store and disclose that information through the Platform.

3. What information we collect

The information we collect depends on how Brightside Connect is used. It may include the following categories of information.

3.1 Account and user information

- Name, business name, role, job title and organisation details.
- Email address, phone number, login details and authentication information.
- User permissions, access role, status, audit logs and usage records.
- Billing, subscription, support and account administration information.

3.2 Staff, worker and contractor information

- Name, contact details, address, emergency contact details and employment type.

-
- Roles, locations, availability, skills, qualifications, certifications and compliance records.
 - Rostered shifts, attendance, timesheet information, pay-related operational data and notes.
 - Documents uploaded by or about staff, including onboarding or compliance documents.

3.3 Participant, client and care-related information

- Name, contact details, address, representatives, emergency contacts and identifiers.
- Support requirements, service categories, plans, funding information, rostered supports and notes.
- Information contained in uploaded documents, reports, incident records, forms, templates and communications.
- Sensitive information or health information where it is entered into the Platform by or on behalf of a customer organisation.

3.4 Technical and usage information

- Device, browser, IP address, access dates and times, pages viewed, actions taken and diagnostic logs.
- Security, audit and system event logs.
- Information collected through cookies or similar technologies on our website or Platform, where applicable.

3.5 Communications and support information

- Emails, messages, support requests, call notes, chat records, feedback and issue reports.
- Information you provide when requesting help, implementation assistance, troubleshooting or support.

4. Sensitive information and health information

Brightside Connect may process sensitive information, health information or care-related information where it is entered into the Platform by or on behalf of a customer organisation. This may include information about disability supports, health needs, care requirements, medication prompts, incident reports, behaviour support, compliance records or other sensitive details.

We only collect or process sensitive information where it is reasonably necessary for providing the Platform and Services, where it is authorised by the customer organisation, where the individual has provided any required consent, or where otherwise permitted or required by law.

Customer organisations are responsible for ensuring that individuals are properly notified and that all required consents, authorisations or lawful bases have been obtained before sensitive information is entered into Brightside Connect.

5. How we collect information

We may collect information directly from you, from customer organisations that use Brightside Connect, from authorised users, from uploaded files and documents, from integrations and third-party systems connected by a customer, from support interactions, and automatically through use of the Platform.

Where information is provided to us about another person, the person or organisation providing the information must ensure they have authority to do so and that the individual has received any required privacy notices.

6. Why we collect, use and disclose information

We collect, use and disclose personal information for purposes connected with providing, maintaining, improving and securing Brightside Connect and related services, including to:

- create, administer and secure user accounts;
- provide access to the Platform, mobile application, modules, tools, templates, integrations and automation features;

-
- support rostering, participant and client management, staff management, document management, compliance tracking, incident reporting, invoicing, pay run preparation, communications and related business administration;
 - provide customer support, implementation assistance, troubleshooting, training and account management;
 - send service-related communications, alerts, reminders, release updates, billing notices and security notices;
 - process SMS, email, in-app and other communications requested or configured by a customer organisation;
 - operate, monitor, secure, back up and improve the Platform;
 - detect, investigate and prevent misuse, unauthorised access, fraud, security incidents or breaches of our terms;
 - comply with legal obligations, regulatory requirements, court orders, law enforcement requests and dispute resolution processes;
 - manage subscriptions, billing, payments, records and business operations; and
 - improve Brightside Connect, including through analytics, quality assurance and product development, using de-identified or aggregated information where appropriate.

7. Artificial intelligence and automation

Brightside Connect may include artificial intelligence, automation, document generation, matching, rostering suggestions, compliance reminders, workflow recommendations, report generation or other assisted tools.

Where these features are used, relevant information entered into the Platform may be processed to generate or assist outputs requested by the customer organisation or authorised user. AI and automation outputs may be incomplete, inaccurate or unsuitable and must be reviewed by the customer organisation before being relied on or sent to a participant, client, employee, regulator or third party.

We do not use customer confidential information or customer data for unrelated purposes. Where we use de-identified or aggregated information to improve Brightside Connect, we take reasonable steps so that individuals are not reasonably identifiable.

8. Communications, SMS and reminders

Brightside Connect may allow customer organisations to send or automate communications, including SMS, email, in-app messages, shift offers, shift reminders, account invitations, compliance reminders, release updates and operational alerts.

Customer organisations are responsible for ensuring that recipients have been properly notified and, where required, have consented to receive communications. Customers are also responsible for the content, timing and lawfulness of communications they configure or send through the Platform.

We may use third-party communication providers to deliver SMS, email or other messages. Those providers may process recipient names, phone numbers, email addresses, message content, delivery metadata and related technical information as necessary to deliver the communication.

9. Integrations and third-party services

Brightside Connect may integrate with third-party services such as accounting platforms, payment providers, SMS providers, email services, calendar systems, cloud storage, government data sources, API services and other tools.

If a customer organisation connects a third-party service, the customer authorises us to access, transmit and process information through that service as necessary to provide the requested integration. Third-party services are governed by their own privacy policies, terms, security practices and data handling arrangements.

We are not responsible for the privacy or security practices of third-party services that are connected or used by a customer organisation, except to the extent required by law.

10. Disclosure of information

We may disclose personal information where reasonably necessary for the purposes described in this Privacy Policy, including to:

- authorised users within the relevant customer organisation;
- service providers who help us host, operate, secure, support, maintain or improve Brightside Connect;
- SMS, email, payment, analytics, hosting, cloud infrastructure, support, security, backup and integration providers;
- professional advisers, insurers, auditors, accountants and legal advisers;
- law enforcement, regulators, courts, tribunals or government bodies where required or authorised by law;
- another person or organisation where you or the relevant customer organisation has authorised disclosure; and
- a purchaser or prospective purchaser in connection with a business sale, restructure, merger or similar transaction, subject to appropriate confidentiality safeguards.

We do not sell personal information to advertisers.

11. Overseas disclosure

Some of our service providers, hosting providers, support tools, communication providers or integration partners may store or process information outside Australia. The countries in which information may be processed can vary depending on the services used and the locations of our providers.

Where personal information is disclosed overseas, we take reasonable steps to use reputable providers and appropriate safeguards, having regard to the nature of the information and the services being provided. Customer organisations should also assess whether connected third-party services meet their own privacy and data governance requirements.

12. Security

We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. Measures may include access controls, authentication, encryption where appropriate, hosting controls, monitoring, backups, logging, system updates and operational safeguards.

No software platform, internet transmission, cloud service or storage system can be guaranteed to be completely secure. Customer organisations and users also have security responsibilities, including protecting login credentials, using appropriate permissions, maintaining device security, training staff, managing exports and promptly removing access for users who no longer require it.

13. Data retention

We retain personal information for as long as reasonably necessary to provide the Platform and Services, meet legal, operational, security, audit, backup, billing and dispute resolution requirements, or as otherwise agreed with a customer organisation.

Customer organisations are responsible for managing retention of records they are legally or operationally required to keep. Following termination or cancellation, customer data may be retained for a limited period for backup, legal, audit, security, dispute resolution or operational purposes before deletion in accordance with our Terms and Conditions or applicable agreement.

14. Access and correction

You may request access to, or correction of, personal information we hold about you by contacting us at admin@brightsideai.com.au.

If your information is held within a Brightside Connect account controlled by a customer organisation, we may direct you to that organisation because it controls the relevant account and data. We may need to verify your identity before responding to a request.

We may refuse access or correction in circumstances permitted by law, including where access would affect another person's privacy, reveal commercially sensitive information, create a security risk, or where the request is frivolous, vexatious or unlawful. If we refuse a request, we will provide reasons where required by law.

15. Privacy complaints

If you have a concern about how we handle personal information, contact us at admin@brightsideai.com.au. Please include enough detail for us to understand and investigate your concern.

We will aim to respond within a reasonable time. If you are not satisfied with our response, you may be able to contact the Office of the Australian Information Commissioner or another relevant regulator, depending on the nature of the issue.

16. Cookies and website analytics

Our website or Platform may use cookies, local storage, analytics tools or similar technologies to operate the service, keep users signed in, remember preferences, secure accounts, understand usage and improve performance.

You may be able to control cookies through your browser settings. Disabling some cookies may affect the functionality of the website or Platform.

17. Children's privacy

Brightside Connect is designed for use by organisations and authorised users and is not directed to children. Customer organisations may enter information about participants or clients who are children where they have the necessary authority, consent or lawful basis to do so and where it is relevant to the services being provided.

18. Changes to this Privacy Policy

We may update this Privacy Policy from time to time. If we make material changes, we will take reasonable steps to notify affected customers or users, such as by email, website notice, in-platform notice or account notification.

The updated Privacy Policy will apply from the date stated at the top of the policy or from another date specified in the notice.

19. Contact

For questions about this Privacy Policy or how personal information is handled, please contact:

Brightside Connect

Email: admin@brightsideai.com.au

Website: <https://brightsideai.com.au/>