Creative Career Nursing Agency
ABN: 59 219 362 119
Registered Office
630 Regency Road, Broadview SA 5083

PRIVACY POLICY

Creative Career Nursing Agency SA (CCNASA)

Version: Version 1
Effective Date: January 2026
Review Date: January 2027

1. Purpose

Creative Career Nursing Agency SA ("CCNASA", "we", "our", "us") is committed to protecting the privacy, confidentiality, and security of personal and sensitive information collected from employees, contractors, applicants, clients, participants, and business partners.

We comply with the requirements of the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), applicable aged care and healthcare regulations, contractual obligations, and industry best practice standards.

This Privacy Policy explains how we collect, use, store, disclose, and protect personal information.

---

2. Information We Collect

CCNASA may collect personal information including:

Applicant Information

- Full name
- Contact details
- Date of birth
- Employment history
- Qualifications and training records
- Professional registrations
- Vaccination records
- Working rights documentation
- Police clearances
- NDIS Worker Screening Checks
- References
- Identity documents

Employee and Contractor Information

- Payroll and taxation information
- Bank account details

- Superannuation details
- Emergency contact information
- Performance and training records
- Rostering and attendance information

Client and Participant Information

- Contact details
- Care requirements
- Clinical information
- Care plans
- Risk assessments
- Service delivery records
- Incident reports
- Consent documentation

Some information collected may be classified as sensitive information under the Privacy Act 1988 (Cth).

CCNASA does not routinely collect photographs, video or audio recordings of clients, participants or staff using personal devices. Any authorised recording undertaken for legitimate business purposes will be managed in accordance with this Privacy Policy, applicable legislation and organisational procedures.

---

3. Why We Collect Information

We collect personal information to:

- Assess employment applications
- Verify qualifications and credentials
- Meet workforce compliance requirements
- Deliver healthcare and support services safely
- Manage employment relationships
- Meet contractual obligations with healthcare providers
- Comply with legal and regulatory requirements
- Protect the safety of clients, participants, staff, and the public

Failure to provide requested information may prevent us from assessing an application or assigning staff to healthcare facilities where compliance requirements apply.

4. Applicant Information Collection

As part of the recruitment process, applicants may be required to upload personal documentation through secure recruitment platforms.

This information is collected to:

- Verify identity
- Confirm professional qualifications
- Confirm registration status
- Conduct compliance checks
- Meet client facility onboarding requirements
- Assess suitability for employment

All information submitted during recruitment is handled confidentially and accessed only by authorised personnel involved in recruitment, compliance, and workforce management.

5. Access Control and Protection of Information

CCNASA implements strict governance and system-based controls to ensure personal and sensitive information is accessed only by authorised personnel and solely for legitimate business purposes.

Governance and Delegation of Authority

We operate under a formal Delegation of Authority framework that defines who may access, edit, approve, and share information.

Access is granted strictly on a need-to-know basis.

Examples include:

- Care staff accessing information required for safe service delivery.
- Coordinators accessing information required to manage placements and services.
- Managers accessing information necessary for operational oversight and compliance.

Access permissions are reviewed regularly and immediately updated following role changes or termination of employment.

6. System Security Measures

Our systems are protected through multiple security controls including:

- Two-factor authentication (2FA)
- Unique user accounts

- Strong password requirements
- Role-based access permissions
- Encryption of data in transit and at rest
- Australian-hosted cloud-based systems where applicable
- Regular security reviews

These controls help ensure information is protected from unauthorised access, misuse, loss, or disclosure.

---

7. Audit Logging and Monitoring

Our systems maintain comprehensive audit trails that record:

- User login activity
- Access to records
- Creation and modification of records
- Information sharing activities

Audit logs may be reviewed to investigate incidents, monitor compliance, and support quality assurance activities.

---

8. Staff Responsibilities

All employees, contractors, and agency personnel are required to:

- Maintain the confidentiality of all personal and sensitive information
- Access information only where required to perform their duties
- Follow company privacy, cybersecurity, and information management policies
- Complete mandatory privacy and data protection training
- Report suspected privacy breaches immediately
- Protect passwords and system credentials from unauthorised use

Personal Recording Devices and Wearable Technology

To protect the privacy, dignity and confidentiality of clients, participants, residents, visitors and staff, employees, contractors and agency personnel must not use or wear any personal device capable of capturing, recording, storing or transmitting images, video or audio while performing work duties, unless expressly authorised by management for a legitimate business purpose.

This includes, but is not limited to:

- Smart glasses

- Smart watches
- Mobile phones
- Tablets
- Cameras
- Wearable cameras
- Audio recording devices
- Any other wearable or electronic recording device

The use of personal devices to photograph, film, record or share any client, participant, resident, visitor, staff member or confidential workplace information is strictly prohibited.

Personal mobile phones may only be used in accordance with organisational policy and must never be used to record, photograph, film or store personal or confidential information relating to clients, participants, residents or the workplace.

Unauthorised recordings or images must not be uploaded, transmitted or shared through social media, messaging applications, cloud storage services or any other electronic platform.

Failure to comply with this policy may result in disciplinary action, including termination of employment or engagement, and may constitute a breach of the *Privacy Act 1988 (Cth)*, applicable South Australian legislation, contractual obligations and professional standards.

All staff are required to sign confidentiality agreements as a condition of engagement.

Failure to comply with privacy obligations may result in disciplinary action, including termination of employment or engagement.

9. Disclosure of Information

We may disclose personal information:

- To healthcare facilities where staff are being placed
- To clients, participants, or authorised representatives
- To support coordinators and allied health providers
- To government agencies and regulators where legally required
- To third-party service providers supporting our operations

Information is shared only:

- With consent;
- Where necessary for service delivery;
- To comply with legal obligations; or

- To protect health, safety, or welfare.

---

10. Secure Transmission of Information

When transmitting personal information, CCNASA uses secure methods including:

- Encrypted email
- Secure file-sharing platforms
- Password-protected documents
- Secure cloud-based systems

Reasonable steps are taken to ensure information remains protected during transmission.

---

11. Data Retention

Personal information is retained only for as long as required by law, contractual obligations, or legitimate business purposes.

Participant and client records are generally retained for a minimum of seven (7) years following completion of services unless a longer period is required by law.

Archived information remains protected through:

- Restricted access controls
- Encryption
- Audit logging
- Secure storage environments

---

12. Secure Deletion and De-Identification

When information is no longer required, CCNASA will:

- Permanently and securely delete electronic records; or
- De-identify information for approved quality improvement, reporting, or statistical purposes where appropriate.

Where third-party systems are involved, confirmation of secure deletion may be obtained.

---

13. Data Breaches

Any actual or suspected data breach is managed in accordance with our Data Breach Response Procedure and the Notifiable Data Breaches Scheme.

Where required by law, affected individuals and the Office of the Australian Information Commissioner (OAIC) will be notified.

---

14. Access and Correction Requests

Individuals may request access to, or correction of, their personal information by contacting us.

Requests will be handled in accordance with applicable privacy legislation.

---

15. Complaints

If you believe your privacy has been breached, you may submit a complaint to:

Privacy Officer
Creative Career Nursing Agency SA
630 Regency Road, Broadview SA
admin@ccnasa.com.au
08) 7226 9656

Complaints will be investigated promptly and responded to within a reasonable timeframe.

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC).