Privacy Policy

Purpose

The purpose of this Privacy Policy is to inform people of how KINNECT abide by the Australian Privacy Principles and the Privacy Act 1988 (Cth) which govern the way private sector organisations collect, use, keep secure and disclose personal information and sensitive information during the provision of services. It also documents how an individual can access and correct their personal information and how we will facilitate or resolve a privacy complaint.

Scope

This Privacy Policy relates to KINNECT Pty Ltd (ACN 114 691 860) and its Related Bodies Corporate (as defined by the provisions of the Corporations Act 2001 (Cth). KINNECT's privacy obligations relate to all systems, departments and employees (incl contractors) in the above stated entities.

State and Territory Legislation

As a Health Service Provider, KINNECT acknowledge the requirements to comply with both State and Territory privacy laws (where they are in place). As an organisation operating in New South Wales (NSW), Victoria (VIC) and the Australian Capital Territory (ACT), KINNECT's privacy policy also takes in to account the applicable privacy legislations as laid out below:

New South Wales (NSW)	• Health Records and Information Privacy Act 2002 (NSW).
Victoria (VIC)	• Health Records Act 2001 (VIC)
Australian Capital Territory (ACT)	• Health Records (Privacy and Access) Act 1997 (ACT)

How we Seek and Manage Consent

At KINNECT, we aim to be clear and respectful about how we collect and use your personal and sensitive information—especially when your consent is required. We seek your express consent before we collect, use, or share your personal or sensitive information as outlined in this policy. Consent is usually captured through:

- An initial discussion with your KINNECT consultant
- A written or digital consent form that outlines the specific uses of your information

By signing the consent form, you are confirming your agreement for the disclosure, transfer, storing or processing of your personal and/or sensitive information, including the potential for cross-border disclosure, use of artificial intelligence and use of data for research purposes. If you're unsure or have concerns about any part of this, we encourage you to speak with your KINNECT representative. In many cases, we can adjust how your information is used, depending on your needs.

Note: Sometimes we may need to collect or share your information without consent—for example, when required by law, or to protect someone's health or safety. We always act in accordance with the Australian Privacy Principles and applicable health laws.

Incapacity to Consent

In situations where you do not have capacity to provide informed consent or make decisions about your health care (such as during a medical emergency), we do not need your consent to disclose your personal information relating to your health to the person who is responsible for your care, usually your legal guardian or doctor.

Withdrawal of Informed Consent

You are able to withdraw or change your consent at any time. This will not affect any of the information that has already been collected or released; however, may limit the services we can continue to offer. If you're considering this, we encourage you to speak with your KINNECT representative so we can explain any implications and work with you on a solution.

Collection of Information

Throughout your engagement with KINNECT, you may be required to provide us with personal and/or sensitive information. KINNECT only collect information that is reasonably necessary for the provision of services for which you have been referred, and in order for us to be able to effectively coordinate services and facilitate the referral objectives and goals of services.

What is Personal Information?

The Privacy Act 1988 (Cth) (Privacy Act) defines "personal information" to mean any information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Types of personal information collected by KINNECT during the provision of services might include (but is not limited to):

- Name
- Contact information
- Employment details
- Financial information
- Identification numbers (Medicare, Passport, Driving Licence etc)
- Location data

What is Sensitive Information?

Sensitive information is a subset of personal information that requires a higher level of protection due to its confidential or personal nature. Given the nature of the work we do, it is likely we will collect sensitive information from you in order to carry out the services provided to you. KINNECT do not collect sensitive information from you without your explicit consent unless a permissible situation arises, as documented in APP3, such as, lessening or preventing a serious threat to life, health or safety or taking appropriate action in relation to suspected unlawful activity or serious misconduct.

The type of sensitive information we may collect about you is dependent on the services provided to you by KINNECT and will be limited to the purpose(s) for which it is collected. Types of sensitive information collected by KINNECT during the provision of services might include (but is not limited to):

- Health information (including physical or mental health, medical history, and any related treatment)
- Racial or ethnic origin
- Membership information (political associations, professional associations, trade unions)
- Criminal record
- Gender identity

General Collection

As much as possible or unless stated otherwise in this Privacy Policy or a notification, we will collect your personal information directly from you. However, depending on the circumstances and the nature of the services we are providing in respect of you, we may also collect your personal information from:

a) a referring medical provider, and independent medical services provider (such as an IME), or other health or medical third party in order to provide our services effectively;
b) an insurer of you or your employer
c) an employer when we have been engaged by your current or prospective employer to conduct health, medical, or drug or alcohol screening or training;
d) other individuals in order to assist you during a medical emergency;
e) when we collect personal information about you from publicly available sources.

Depending upon the reason for requiring the information, some of the information we ask you to provide may be identified as mandatory or voluntary. You may choose not to provide the requested mandatory information; however, this will impact on the ability for KINNECT to continue to provide effective services and may impact the ability to provide any services at all.

When you engage in certain activities, such as filling out a survey or sending us feedback, we may ask you to provide certain information. It is completely optional for you to engage in these activities.

KINNECT may record calls for the purposes of training and quality assurance. If you do not wish for your call to be recorded, you are able to opt out by following the prompts.

Anonymity and Pseudo-anonymity

Given the sort of services we provide, it is generally not practical for KINNECT to correspond with you, or provide our services to you, in an anonymous manner or when you use a pseudonym. Your personal information may be required in order to provide you with our services or to resolve any issue you may have.

Notification of Collection

At or before the time that KINNECT collects personal information about you, or as soon as practicable after collection, KINNECT will whenever reasonably practicable, take steps to notify you or otherwise ensure that you are aware of the matters that are required by APP 5 including but not limited to:

a) The facts, circumstances and purpose of collection
b) The possible adverse consequences (if any) for you if the personal information is not collected
c) Whether the collection is required or authorised by law
d) KINNECT's usual practices in relation to use and disclosure of personal information, including cross-border disclosure
e) How you can access or correct your details

Unsolicited Personal Information

In the event we collect personal information from you, or a third party, in circumstances where we have not requested or solicited that information (known as unsolicited information), and it is determined by KINNECT that the personal information could not have been collected under APP3, KINNECT will destroy or de-identify the personal information as soon as practicable. In the event that the unsolicited personal information collected is in relation to potential future employment with KINNECT, such as your CV, resume or candidacy related information, and it is determined by KINNECT (in its absolute discretion) that it may consider you for potential future employment, KINNECT may keep the personal information on its human resource records.

Cookies and IP Addresses

Our website uses cookies and similar tracking technologies to enhance user experience, monitor website traffic, monitor trends and support marketing efforts. In most cases, a cookie does not identify you personally but may identify your internet service provider, IP address or computer. You can manage your cookie preferences through your browser settings. By using our website, you consent to our use of cookies in accordance with this Privacy Policy.

Storage of Information

How we Hold your Personal Information

Once we collect your personal information, this is held and stored securely on infrastructure owned or controlled by us or with a third-party service provider who have taken reasonable steps to ensure they comply with the *Privacy Act 1988* (Cth). Where we have collected Personal Information in order to provide services, this information is stored securely in our Carelever platforms. KINNECT uses Amazon Web Services (AWS) to host this platform, with data and hosting services being stored in the Asia Pacific Region located in Sydney, NSW.

Further details on Carelever Security can be found in the Carelever Platform Security Policy.

Use and Disclosure of Information

Purpose for Disclosure of Information

KINNECT will only use or disclose your personal information for the primary purposes for which it was collected or as consented to by you, unless an exception under the Privacy Act applies to that disclosure or use.

This would include (but is not limited to):

a) when it would be reasonably expected that we would use or disclose the information for the secondary purpose and, for sensitive information, the secondary purpose is directly related to the primary purpose;
b) if we reasonably believe that the use or disclosure is necessary to lessen or prevent a serious or imminent threat to an individual's life, health or safety or to lessen or prevent a threat to public health or safety;
c) if we have reason to suspect that unlawful activity has been, or is being, engaged in; or
d) if it is required or authorised by law.

At or around the time we collect personal information from you, we will endeavour to provide you with a notice which details how we will use and disclose that specific information. We set out some common use and disclosure instances below:

Uses

- Verification of Identity
- Delivery of services
- General administrative and security use
- General marketing and consumer analytics
- Administration and performance monitoring use
- Background checks for the purpose of assessing candidate suitability for a role
- Research

Disclosures

- In order to be able to effectively perform the service we provide to you and as documented in the consent form.
- Relevant referral sources (e.g. compensation bodies, employers etc).
- As required or authorised by law
- Service providers (including IT service providers and consultants) who assist KINNECT in providing our products and services.
- Related bodies corporate of KINNECT (including related entities).
- Third parties in connection with the sale of any part of KINNECT's business or a company owned by a KINNECT's entity.
- Relevant superannuation companies
- Government agencies such as The Australian Taxation Office, Centrelink and Child Support Agency
- Service providers (including IT service providers and payroll providers), if any
- Recruitment agents used in connection with your application with us
- Third party parties in connection with obtaining any background checks, reference checks, pre-employment screening

Cross Border Disclosures

The Privacy Act 1988 requires us to take steps as are reasonable in the circumstances, to ensure that any recipients of your personal information outside of Australia do not breach the privacy principles contained within the Privacy Act 1988. In some cases, your personal information may be accessed by KINNECT personnel, service providers, or technology partners located outside Australia, such as for technical support, software development, quality assurance, or system maintenance. This includes access from countries such as the Philippines where offshore personnel are engaged through Shore360 Pty Ltd (and its related Philippine entities) as an Employer of Record, and New Zealand which are subject to contractual and security controls. Location specific access may also be granted to team members in other countries following a full security review by the IT team and approval by the CEO, as business needs arise.

Such access is limited to the extent necessary to support KINNECT's services and operations, and they are only allowed access to information under strict conditions. KINNECT will:

- Limit the ability for overseas team members to download and access information via use of encryption and Cloud PC infrastructure,
- Ensure that any overseas recipient of your personal information is subject to contractual obligations requiring them to comply with privacy standards substantially similar to the Australian Privacy Principles (APPs); or

- Obtain your informed consent before granting such access; or
- De-identify the information before it is accessed, such that it no longer falls within the definition of personal information.

In providing this consent, you understand and acknowledge that countries outside Australia do not always have the same privacy protection obligations as Australia in relation to personal information. However, KINNECT will take steps to ensure that your information is used by third parties securely and in accordance with the terms of this Privacy Policy. Where personal information is disclosed or accessed overseas, KINNECT remains accountable for that information in accordance with the Privacy Act 1988. If we ever discover a privacy breach - including one overseas - we'll act quickly to inform you and help resolve the issue.

Where stipulated by legislation or a contractual agreement that offshore access is restricted, KINNECT will manage data related to these customers via onshore personnel only.

Access to your Personal Information

Under the Australian Privacy Act 1988 (Cth) and Australian Privacy Principle (APP) 12 you have the right to request access to your personal records held by KINNECT, and for KINNECT to respond within a reasonable timeframe. However, access may be refused in limited circumstances, such as where disclosure would pose a serious threat to health, breach another person's privacy, or interfere with law enforcement activities.

Data Security and Quality

KINNECT have taken steps to help secure and protect your personal information from unauthorised access, use, disclosure, alteration, or destruction including, but not limited to:

a) Restricting access to personal and sensitive information in our systems based on the principle of least privilege
b) Multifactor authentication processes
c) User activity monitoring

However, KINNECT acknowledge that we cannot guarantee the security of all transmissions or personal information, especially where human error is involved or malicious activity by a third party. KINNECT will take reasonable steps to:

a) make sure that the personal information we collect, use or disclose is accurate, complete and up to date;
b) destroy or permanently de-identify personal information if it is no longer needed for its purpose of collection.

Data Accuracy

The accuracy of personal information depends largely on the information you provide to us, so we recommend that you:

a) let us know if there are any errors in your personal information; and
b) keep us up to date with changes to your personal information (such as your name or address).

You are entitled to edit and correct personal information where that information is inaccurate, out of date, incomplete, irrelevant or misleading. If you would like access to or correct any records of personal information we have about you, you are able to access and update that information by contacting us via the details set out at the bottom of this document.

Use of Artificial Intelligence (AI)

KINNECT implement a people first, AI assisted approach to its operations utilising with the aim to enhance service delivery while maintaining a human-centered approach. KINNECT does not use AI to make automated decisions about you, the services you are being provided or your eligibility for services. AI is never used to make clinical decisions; outputs are reviewed and validated by qualified personnel before being used in a clinical or operational setting.

KINNECT uses a range of secure, enterprise-grade platforms including Microsoft Co-Pilot (within Microsoft 365 and Azure environments) and ChatGPT Enterprise to support:

- Operational activities – preparing service quotes, drafting emails and meeting materials, and recording or transcribing calls and training sessions
- Reporting and documentation – generating draft reports, structuring content, and supporting quality assurance activities (e.g. audits, file reviews)
- Medical and health information support – assisting with the summarisation or organisation of clinical data.
- Compliance and governance – monitoring adherence to regulatory and legislative requirements and processes
- Data analysis and insights – extracting, summarising, and analysing data to support research and service improvement

KINNECT only uses AI technologies in ways that ensure compliance with its obligations under the *Privacy Act 1988 (Cth)* and the *Australian Privacy Principles*. This includes:

- Only processing identifiable personal or sensitive information where we have explicit consent
- Only processing identifiable personal or sensitive information in a secure Australian environment such as Microsoft Azure (Australia East or Southeast regions)
- Where information has been obtained that could not otherwise be collected under APP3, ensuring this is destroyed or de-identified.
- Only using information for the primary purpose for which it was collected, unless we have explicit consent

If consent is not provided for use of personal information within AI, only information that has been de-identified or pseudonymised — and cannot reasonably be used to identify you — will be used for AI-assisted tasks. This means your name, contact details, and other identifiable fields will be removed or masked before data is submitted to AI systems.

When new AI systems are introduced, or existing ones are significantly changed, we assess their privacy, security, and ethical implications through our internal governance processes, including conducting Privacy Impact Assessments where appropriate.

Direct Marketing

What is Direct Marketing?

Providing you with information and telling you about our products, services or events or any other direct marketing activity (including third party products, services, and events) which we consider may be of interest to you, whether by post, email, SMS, messaging applications and telephone.

Inferred Consent and Reasonable Expectations of Direct Marketing

Where you have provided consent, including inferred or implied consent (e.g. not opting out where an opt-out opportunity has been provided to you), or if it is within your reasonable expectation that we send you Direct Marketing Communications given the transaction or communication you have had with us, then KINNECT may use your personal information for the purpose of sending you Direct Marketing Communications which we consider may be of interest to you. We do not use sensitive information to send you Direct Marketing Communications without your express consent.

Opt-Out

If at any time you do not wish to receive any further Direct Marketing Communications from us or others, you may ask us not to send you any further information about products and services and not to disclose your information to other organisations for that purpose. You may do this at any time by using the “unsubscribe” facility included in the Direct Marketing Communication or by contacting us via the details set out at the bottom of this document.

Related Policies

- Acceptable use of Information Technology Policy
- Carelever Information Policy
- Carelever Security Policy
- Credit Reporting Policy
- Data Breach Management Policy

- Data Retention Policy
- General Information Security Policy
- Identify and Access Control Management Policy
- Mobile Device Security Policy
- People IT Security policy
- Social Media Policy
- Use of AI Tools Policy

Complaints

Privacy Complaints

If you have any concerns or complaints about the manner in which your personal information has been collected, used or disclosed by us, we have put in place an effective mechanism and procedure for you to contact us so that we can attempt to resolve the issue or complaint

We will ensure that all complaints are dealt with in a reasonably appropriate timeframe so that any decision (if any decision is required to be made) is made expeditiously and in a manner that does not compromise the integrity or quality of any such decision.

Please see the provisions of our Credit Reporting Policy if you wish to make a complaint in relation to our handling of your credit information.

Steps we Take to Resolve a Complaint

In order to resolve a complaint, we:

a) will liaise with you to identify and define the nature and cause of the complaint;
b) may request that you provide the details of the complaint in writing;
c) will keep you informed of the likely time within which we will respond to your complaint; and
d) will inform you of the legislative basis (if any) of our decision in resolving such complaint.

Register of Complaints

We will keep a record of the complaint and any action taken in a Register of Complaints.

Escalation to the OAIC

If you are not satisfied with how we handle your privacy complaint, you may refer your complaint to the Office of the Australian Information Commissioner (OAIC). The OAIC is an independent body that can investigate privacy concerns under the Privacy Act 1988 (Cth). You can contact the OAIC using the following details:

- Website: www.oaic.gov.au
- Telephone: 1300 363 992
- Email: enquiries@oaic.gov.au
- Post: GPO Box 5288, Sydney NSW 2001

Modifications and Updates

We reserve the right to modify our Privacy Policy as our business needs require. We will take reasonable steps to notify you of such changes (whether by direct communication or by posting a notice on our website). If you do not agree to our continued use of your personal information due to the changes in our Privacy Policy, please cease providing us with your personal information and contact us via the details set out below.

We recommend that you keep this information for future reference.

Contacting KINNECT

If you have any concerns or complaints about the manner in which we have collected, used or disclosed and stored your personal information, please contact us:

Telephone:	(07) 3391 2623
Email:	Privacy@kinnect.com.au
Address:	PO Box 8264 Woolloongabba Qld 4102