Privacy Policy

HR+ is committed to protecting and upholding the right to privacy of clients, staff, participants, board members and external stakeholders. In particular HR+ is committed to protecting and upholding the rights of clients to privacy in the way we collect, store and use information about them, their needs and the services we provide them.

HR+ requires staff members to be consistent and careful in the way they manage what is written and said about individuals and how they decide who can see or hear this information.

HR+ will ensure that:

- It meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients and organisational personnel.
- Clients are provided with information about their rights regarding privacy.
- Clients and organisational personnel are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature.
- All staff members understand what is required in meeting these obligations.
- It will adhere to all requirements imposed under the *Privacy Act 1988*, including the requirements imposed by the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, to strengthen the protection of personal information.

In line with this policy, HR+ conforms to the *Privacy Act (1988)* and the Australian Privacy Principles which govern the collection, use and storage of personal information.

This policy details the way in which personal information is collected, used, stored, disclosed and destroyed by the NDIS Team within HR+ in accordance with these privacy principles and will apply to all records, whether hard copy, electronic, containing personal information about individuals, and to interviews or discussions of a sensitive personal nature.

Definitions

Personal Information refers to information that is specific to an individual and could identify that individual.

Sensitive Information is a specific type of personal information that is sensitive in its nature and attracts a higher level of privacy protection than other personal information. Sensitive information can include:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- some aspects of biometric information

Procedures

Collection of Personal Information

In general, personal information will be collected directly using service agreements, client record keeping, and via emails and phone conversations. Whenever HR+ collects information, the purpose of collection will be explained as well as how the information will be used and who it might be provided to. Generally, information is collected for the purpose of:

- management of service to individuals
- service monitoring, evaluation and reporting (de-identified information only is used for this purpose)

- meeting the reporting requirements of the NDIA

If unsolicited information is received which is not information that HR+ require for the purpose it has been provided, HR+ will destroy the information.

Consent must be obtained when collecting personal information that is deemed sensitive. Consent is collected in the process of completing a service agreement. Consent must be informed whereby the individual in question understands the consequences of giving or not giving consent and HR+ staff have clearly explained how they will handle the relevant information.

Consent is voluntary and should include the option not to consent, including an explanation of potential outcomes should a person refuse to consent. In the case of support coordination or plan management, a refusal to provide consent to collect and store information is likely to significantly impact the service provided.

Consent must be current and specific. Consent cannot be assumed to continue indefinitely. HR+ staff will ensure that when asking for consent, they explain the reason for their request (as specific as possible) and that a timeframe is provided suitable to the collection and usage of the relevant information.

At times, personal information may be collected from a third party, or publicly available source, but only if the individual has consented to such collection or would reasonably expect HR+ to collect their information in this way. A third party might include, but is not limited to, regulatory bodies, other providers, or the NDIA.

The types of personal information collected might include:

- Full name
- Contact details e.g., phone, email, residential and postal address, emergency and/or primary contacts
- Demographic information e.g., age, date of birth, gender, occupation
- Sensitive information including health and disability information
- Information relating to services and supports provided through the NDIS
- Details of carers or support persons

HR+ will only use sensitive information for a secondary purpose if it is directly related to the primary purpose.

Client personal information might be shared with regulatory and funding bodies including the NDIA. Information will also be shared with other service providers as required but opportunity is given for the client to specify who this will include. Auditors will also be given access to client information unless a client opts out.

Storage of information

HR+ is committed to taking all reasonable steps to ensure that the information provided to us is secure. Information is held electronically on HR+'s cloud-based Client Relationship Manager (CRM). Access to information is limited to the personnel with the correct authorisation and only as many staff members as necessary are provided with access to client information. All HR+ staff members sign a non-disclosure agreement upon employment. All paper-based records are held only long enough to electronically store and then they are shredded. Where staff leave the organisation their access to data is removed. HR+ takes all reasonable measures to protect personal information from unauthorised access, improper use, disclosure, unlawful destruction and accidental loss. Should a breach occur, staff follow the steps outlined in the **Data Breach Response Plan** using the **Data Breach Incident Report Form**.

Access to information

HR+ acknowledges the rights of individuals to have access to their personal information and to request amendments to this information. Clients are encouraged to update their information as it changes to maintain the currency and accuracy of HR+ records. An individual may request details of personal information that we hold about them in accordance with the Privacy Act 1988 (Cth). If they would like a copy of the information or believe that any information we hold is inaccurate, out of date, incomplete, irrelevant, or misleading, this

should be addressed in writing to HR+. For a person to request a copy, or a correction, of their personal information they should contact HR+ (info@hrplus.com.au or 0363328600).

HR+ reserve the right to refuse to provide an individual with their information in certain circumstances set out in the Privacy Act.

HR+ can refuse to give a person access to their personal information if:

- It may threaten their own or someone else's life, health, or safety
- It may impact someone else's privacy
- Giving access would be unlawful

If giving the person certain information would impact someone else's privacy, HR+ may de-identify areas of the information and provide the remainder. If it's not possible to give information directly to someone because of a concern for their health and safety, then we may give access through an agreed third-party.

Destruction of information

HR+ will only retain information for as long as the information is required to fulfil the purpose it was collected for and for any time period legally required thereafter. Generally, personal information is required while a client is accessing HR+ support coordination or plan management services. Information will then be retained for the legal time period relevant to the type of information, before being destroyed with the assistance of Information Technology providers used.

Complaints

If an individual has a complaint about the way in which their information has been collected, stored, disclosed or used by HR+, please refer to HR+'s **Complaints Policy** for complaints procedure.

Record of policy development		
Version	**Date approved**	**Date for review**
V3.2	23/11/2023	23/11/2024

Responsibilities and delegations	
This policy applies to	All HR+ staff, clients and stakeholders associated with the NDIS Team. It relates to the collection, storage, use, disclosure and disposal of all personal information handled by the HR+ NDIS Team.
Policy approval	CEO

Policy context – this policy relates to:	
Standards	NDIS Practice Standards, specifically standards 1.3; 2.4
Legislation	Privacy Act 1988 (Cth) Privacy Amendment (Notifiable Data Breaches) Act 2017 Australian Privacy Principles
Organisation policies	Record Management Policy Complaints Policy and Procedure Data Breach Response Plan
Forms, record keeping, other documents	Service Agreement Complaints Form Data Breach Incident Report Form Easy English Complaints Brochure Client Charter