# Intereach Privacy Policy

| | | | | | |
|---|---|---|---|---|---|
| **Applies to** | For the purpose of this document, the term "Worker" applies to all employees, volunteers, contractors, students and directors and Family Day Care (FDC) Educators. | | | | |
| **Definitions** | Refer to Schedule of Definitions: *employees, employee records* | | | | |
| **Version** | 8.0 | **Date approved** | 11/11/2025 | **Next review date** | 11/11/2028 |

## 1. Policy Statement

Intereach is committed to maintaining a person's right to privacy by upholding the Australian Privacy Principles (APP) and complying with the Privacy Act 1988 (Cth) and other relevant regulations, legislation and contractual requirements.

Although the Privacy Act does not apply to employee records being used for employment related purposes, Intereach will endeavour to follow best practice as guided by the Australian Privacy Principles.

Intereach collect personal and sensitive information:

- with the prior knowledge and consent of the person (or their legal representative);
- in a fair, non-intrusive and lawful way;
- only if necessary for the function of the service or organisation;
- without intrusion into areas of a person's life that are irrelevant to the services provided;
- directly from the person, where practical and appropriate, rather than a third party;
- after informing the person why the information is being collected and how it will be used; and,
- in an environment where confidentiality can be maintained.

Intereach ensures the effective storage, backup, retrieval, archiving and retention of electronic and printed organisational data, to maintain business continuity and compliance with privacy and record retention obligations and other relevant regulations, legislation and contractual requirements including mitigation and notification obligations where a privacy breach occurs.

Intereach considers privacy breaches can have serious consequences and have robust systems and procedures in place to identify and respond effectively when a breach is identified.

## 2. Objective

The objective of this policy is to outline rights and responsibilities regarding the collection, handling, security, retention, accuracy and access to personal, sensitive and confidential information.

## 3. Definitions

- **Personal information** refers to information or an opinion that identifies an individual. This may include a person's name, address, photograph, contact details, date of birth, employment details or any information where the person is reasonably identifiable.
- **Sensitive information** is a subset of personal information and may include a person's cultural or ethnic origin, health information (such as disability, vaccination evidence or use of health services), religious beliefs, political opinions, sexual orientation, or criminal record.
- **Confidential information** refers to other information that Intereach informs employees and FDC educators is to be kept private or could reasonably be assumed to be. This may include organisational financial and governance information, pending tender applications, employee information and records and the intellectual property of the organisation.

# 4. Responsibilities

It is the responsibility to the Compliance, Safety and Risk Manager, as the assigned Privacy Officer to:

- ensure that all workers are familiar with the Privacy Policy and administrative procedures for handling personal information;
- ensure that service users and other relevant persons are provided with information about their rights regarding privacy; and,
- ensure the handling any queries or complaint about a privacy issue is managed in accordance with organisational policies and procedures.

It is the responsibility of all workers to:

- sign the Intereach Privacy and Confidentiality Agreement prior to employment or registration;
- comply with this policy; and,
- notify their Manager or the Quality Team as soon as a suspected data breach has been identified.

# 5. Policy

## 5.1. Collection of Information

Intereach collect and hold information which is reasonably necessary for the organisation to conduct its usual activities and operations, including developing and delivering services, evaluating outcomes, sharing stories through marketing and conducting research. The kind of information collected and held includes (but is not limited to) personal information about participants, service users, students, volunteers, Directors, FDC educators, prospective workers, contractors and providers (including associated providers).

When interacting with Intereach, a person can choose to be anonymous or use a pseudonym, except where it is required or authorised by law to deal with identified individuals, or it is impracticable to deal with individuals who have not identified themselves.

If we do not collect necessary personal information, we may not be able to provide support or services to participants, service users, employees, contractors and providers (including associated providers).

### 5.1.1. The kinds of personal information collected

The types of personal information that Intereach collect includes:

- name, contact details, date of birth and age;
- gender, details about participants physical and mental health, including disabilities;
- information about participant's support requirements, including details of family and other relationships;
- details of feedback or complaints about services provided by us (either directly or indirectly);
- details of interactions, including any contact we have in person, by email, online or on the telephone;
- images of people in photographs or film;
- bank account details; and,
- employee records.

### 5.1.2. How is personal information collected

Intereach may collect information in a number of circumstances, including when a person:

- is required to provide consent to engage with Intereach in a service, activity or event;
- provides feedback or requests information from Intereach;
- applies for a job, work placement or volunteer position;
- makes a donation; or,
- joins a mailing or contact list.

Intereach often collect personal information from people directly, or from people who are authorised to represent them

Sometimes personal information is collected from a third party if the person has consented, been told of this practice, or would reasonably expect Intereach to collect the information in this way. Examples of this include but are not limited to, collecting information from:

- a healthcare service, such as a residential care facility, which is managing a participant's care;
- referees for prospective employees;
- internet service providers for the purposes of targeted marketing initiatives.

Intereach will seek consent before taking photographs and recordings of individuals using or participating in our services, programs or facilities and before publishing information that identifies an individual in any printed, electronic, video or audio publications.

Personal information is collected about employees and prospective employees in order to conduct employment and employment-related activities such as payroll services, recruitment and selection, performance management, reporting and work health and safety.

#### 5.1.3. How personal information is stored

Intereach stores Personal Information in a variety of formats including, but not limited to:

- databases;
- hard copy files;
- personal devices, including laptop computers;
- third party storage providers such as cloud storage facilities; and,
- paper based files.

#### 5.1.4. How is personal information kept secure

Intereach takes all reasonable steps to protect the personal information we hold from misuse, loss, unauthorised access, modification or disclosure.

These steps include, but are not limited to:

- restricting access and user privilege of information by type of worker, depending on their role and responsibilities;
- ensuring workers do not share personal passwords;
- implementing physical security measures around the buildings and grounds to prevent break- ins;
- ensuring our IT and cyber security systems, policies and procedures, are implemented and up to date;
- ensuring workers comply with internal policies and procedures when handling the information;
- undertaking due diligence with respect to third party service providers who may have access to personal information, including customer identification providers and cloud service providers, to ensure as far as practicable that they are compliant with the APPs or a similar privacy regime;

- the destruction, deletion or de-identification of personal information we hold that is no longer needed or required to be retained by any other laws.

#### 5.1.5. How personal information is disposed of

Intereach will retain personal information for as long as it is needed for the purpose for which it was obtained and in order to comply with legal, regulatory, financial and administrative requirements. Please request a copy of the Intereach *Data Retention and Security Policy* for more detail.

When a person's personal information is no longer needed for the purpose for which it was obtained, Intereach will take reasonable steps to destroy or permanently de-identify it. This includes secure shredding and disposal of hard copy information and permanent deletion of electronic information.

### 5.2. How Intereach uses and discloses personal information

Intereach will use the personal information collected to help provide services or support to a person where explicit consent has been obtained for example through the completion of a Service Consent Form, or implicitly consented through an enquiry received by phone or email.

Consent must be current and reviewed at least every two years. If consent to share information has not been received within the previous two years, explicit consent must be obtained and updated before any information can be disclosed.

Where a participant lacks the capacity to consent to the use of their personal information, we will seek consent from their representative in accordance with Commonwealth, state and territory guardianship laws

#### 5.2.1. Disclosure of personal information

Except for the examples listed below, personal information is disclosed with third parties, such as government agencies and other service providers, with the consent of the person (or their legal representative) and where necessary for the effective provision of service and/or as required by regulation, contract or legislation. Consent may be gained on enrolment or engagement with a service and/or through the completion of an Information Exchange Consent Form.

Intereach will always try to obtain consent before disclosing information to a third party but are permitted to share information with government agencies and non-government organisations without a person's consent if:

- there are concerns about the safety, welfare and wellbeing of children and young people, for example, as mandatory reporters, Intereach are required by law to report to Child Protection in NSW and Victoria if it is suspected, on reasonable grounds, that a child or young person is at risk of significant harm;
- a request for information under Chapter16A Request or Section 248 of the Children and Young Persons (Care and Protection) Act 1998 for statutory interventions;
- a person is an Intereach Worker and there have been allegations against that person of sexual offence or misconduct to, or in the presence of, a child or any other form of harm or neglect of a child; or
- it is essential to lessen or prevent a serious threat to the life, health or safety of any person, or to public health or safety, or to take appropriate action about suspected unlawful activity or serious misconduct.

As a requirement of the funding of our services, Intereach may be required to share de-identified information (where personal identifiers such as name and address have been

removed) about people receiving services with the government agency accountable for the service.

In accordance with contractual, regulatory and legislative requirements, Intereach are obligated to report serious incidents and complaints, which may contain personal information.

#### 5.2.2. Protection of personal Information

To ensure the security and safety of the people we work with Intereach will refrain from granting access to documents that might reveal personal information about other individuals.

This includes information contained in the following documents:

- assessments or evaluations for delivery of educational programs;
- accident, injury, trauma and illness records;
- medication records;
- attendance records;
- enrolment records.

Intereach will obtain written consent before any personal information is disclosed that may identify the following people:

- a parent of a child enrolled at the service, other than the person requesting the documentation;
- a person required to be notified of an emergency if a parent cannot be contacted;
- an authorised nominee of the child;
- a person authorised to consent to medical treatment or the administration of medication to a child;
- a person authorised to authorise an educator to take a child outside the service premises; and,
- a person authorised to authorise the service to transport a child or arrange transportation of a child.

#### 5.2.3. Disclosure of personal information overseas

In order to ensure that any third-party agencies who have access to a person's personal information, as outlined above, abide by the Australian Privacy Principles, a person's personal information will not be disclosed nor shared directly or indirectly with any agency based outside of Australia.

### 5.3. Data Breaches

The Notifiable Data Breach Scheme requires organisations to notify particular individuals and the Office of the Australian Information Commissioner (OAIC) if an 'eligible data breach' occurs. A data breach is eligible if it's likely to result in serious harm (psychological, emotional, physical, reputational or other forms of harm) to any of the individuals to whom the information relates.

Intereach recognise data breaches may fall into two (2) primary categories, serious (eligible) and minor. To ensure that breaches are responded to in an appropriate timely manner the *Data Breach Response procedure* must be followed. Minor breaches are those that are rectified quickly and individuals are not at risk of serious harm. Eligible data breaches will result in immediate notification (within 72 hours where possible) to individuals affected and to the OAIC.

## 5.4. Accessing and correcting personal information

Individuals have a right under the Privacy Act to access personal information Intereach hold about them. Individuals may also request corrections of any personal information that is held about them, where they believe the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

To request access or seek correction of personal information, individuals may contact Intereach by phone, email or in person and provide identification to prove their identity to facilitate the request. Intereach will respond to requests within a reasonable period of time (usually 30 days).

The APPs outline circumstances in which Intereach may refuse to give a person access or decline to correct personal information. If an access request to personal information is denied, reasonable steps are taken to give the person access to the information in an alternative form. A person will be provided with a written notice setting out the reasons for refusal, and how they can lodge a complaint about the decision.

## 5.5. Complaints

If a person believes that there has been a breach in their privacy, they can contact Intereach directly or via the Intereach website. Details on how to make a complaint are set out in the Feedback and Complaint Policy, available on the Intereach website.

Intereach are committed to a prompt and fair resolution of complaints and will ensure that a person's complaint is taken seriously and investigated. In all cases, the person will be informed of the progress and outcome of the complaint.

If a person is not satisfied with the way a complaint has been handled, they may contact the Office of the Australian Information Commissioner (OAIC). A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted.

Contact details OAIC:

**Telephone** 1300 363 992
**Email** enquiries@oaic.gov.au
**Post** GPO Box 5218, Sydney NSW 2001

## 5.6. Our website and social media channels

Intereach uses social media platforms including Facebook, LinkedIn, Instagram, Twitter, YouTube, and Google to tailor the information delivered on social media and the Intereach website to the preferences of Intereach's audience.

### 5.6.1. Website Cookies

We may collect information based on how individuals use our website. We use "cookies" and other data collection methods to collect information on website activity such as the number of visitors, the number of pages viewed and the internet advertisements which bring visitors to our website. This information is collected to analyse and improve our website, marketing campaigns and to record statistics on web traffic. We do not use this information to personally identify individuals.

| 6. Context | |
|---|---|
| **6.1. Standards or other external requirements** | Australian Privacy Principles<br>Information Privacy Principles (Vic)<br>National Quality Standards<br>Aged Care Strengthened Quality Standards<br>Aged Care Statement of Rights |
| **6.2. Legislation or other requirements** | Aged Care Act 2024 (Cth)<br>Aged Care Rules 2025<br>Privacy Act 1988 (Cth)<br>Privacy and Other Legislation Amendment Act 2024<br>Education and Care Services National Regulations (NSW)<br>Privacy and Data Protection Act 2014 (Vic)<br>Freedom of Information Act 1989 (NSW)<br>Children and Young Persons (Care and Protection) Act 1998 Chapter 16A<br>Privacy and Personal Information Protection Act 1998 (NSW) |
| **6.3. Reference Internal documents** | Code of Conduct Policy<br>Feedback and Complaint Policy<br>Data and Security Retention Policy<br>Child Safe Policy<br>Child Protection Procedure<br>Privacy and Confidentiality Agreement<br>Media Consent Form<br>Service Consent Form<br>Information Exchange Consent Form<br>Data Breach Response Procedure<br>Information Sharing Guidelines<br>Incident Management Policy |

## 7. Document control

| Version | Date approved | Approved by | Next review date |
|---|---|---|---|
| 1.0 | 2009 | CEO | 2012 |
| 2.0 | January 2012 | CEO | January 2015 |
| 3.0 | December 2014 | Combined Leadership Group | December 2017 |
| 4.0 | March 2017 | Combined Leadership Group | March 2020 |
| 5.0 | January 2018 | CEO (minor change re. consent renewal) | March 2020 |
| 6.0 | July 2021 | Board | July 2024 |
| 6.1 | 30 September 2021 | Carolyn Holness, Senior Manager, WHS & Quality (Minor change) | 30 July 2024 |
| 7.0 | 09 February 2024 | Quality and Risk Governance Group | 09 February 2027 |
| 8.0 | 11 November 2025 | Quality, Risk and Performance Governance Group | 11 November 2028 |