Purpose

Estia Foundation of Australia respects your privacy and protects the confidentiality of your information. This policy explains what information we collect, how we use and protect it, and how you can access your information, request a correction or raise a concern. Respecting privacy supports each person's dignity, choice and trust in our services.

Who this policy applies to

This policy covers personal and sensitive information Estia handles about participants, families, representatives, workers, volunteers, applicants, donors and other people who contact us. It applies to directors, committee members, employees, contractors, volunteers, students and authorised third parties, and to information in paper, electronic, photographic, recorded and spoken form.

Policy objectives

1. Collect only information we need

We collect information reasonably necessary to provide and manage support, meet legal obligations and operate Estia. This may include names, contact details, dates of birth, emergency contacts, representative arrangements, NDIS details, service agreements, billing information, support notes and incident records. Where relevant, we collect health and disability information, medication and support needs, cultural or communication preferences and consent records. Employment-related records may include qualifications, screening, payroll and recruitment information.

2. Explain how and why information is collected

We usually collect information directly from you through conversations, forms, enquiries, service delivery and correspondence. Where appropriate and lawful, we may collect it from an authorised representative, health professional, referring provider, funder or government agency. We explain the purpose, relevant disclosures and consequences of not providing requested information through a collection notice or discussion. We deal with unsolicited information according to law.

3. Support consent and individual choice

We seek informed consent for collecting sensitive information unless the law permits or requires collection without consent. We explain requests in a way you can understand and check a representative's authority before relying on their consent. You may withdraw consent for future optional uses, such as publicity, at any time. Where lawful and practical, you may contact us anonymously or use another name. Some information is necessary to provide safe support, process payments or meet legal duties; we will explain any effect of withholding it.

Policy objectives continued

4. Use and share information lawfully

We use information to plan and deliver supports, communicate with you, manage safety, process funding and payments, respond to complaints, train and supervise workers, and meet reporting and audit obligations. We use or disclose information for its collected purpose, with consent, or otherwise as permitted or required by law. For secondary purposes, we apply the relevant privacy rules, including the stricter requirements for sensitive information. We share only what is reasonably necessary.

Recipients may include authorised workers and service providers, health professionals and emergency services, representatives you authorise, plan managers, the NDIA, the NDIS Commission, auditors, insurers, professional advisers and other authorities where lawfully required or permitted. Family relationships alone do not give automatic access to an adult participant's information. We do not sell personal information. Optional photographs, stories and promotional material require specific consent, separate from consent to receive supports.

5. Keep information secure and confidential

We hold information in controlled electronic systems and secure physical records. We take reasonable steps to prevent misuse, interference, loss and unauthorised access, disclosure or alteration through access controls, secure storage, staff training and appropriate supplier arrangements. Workers may access information only for authorised duties and must keep it confidential during and after their work with Estia. Confidential matters must not be discussed in public or posted on personal social media.

Records are retained for applicable legal, contractual and service requirements. When information is no longer needed and retention is not required, we take reasonable steps to securely destroy it or permanently de-identify it. We take reasonable steps to keep information accurate, complete, current and relevant. Please tell us when your details or support needs change.

6. Protect information handled through technology

We assess privacy and security when selecting or changing systems and service providers. Where an arrangement involves disclosure to an overseas recipient, we apply applicable cross-border privacy safeguards. We will explain relevant overseas disclosures, including recipient countries where practicable, in the collection information for that arrangement. You can ask the Privacy Officer about the location and handling of your records.

Information you submit through website enquiries is handled under this policy. Please avoid sending unnecessary health or identity documents through an enquiry form or ordinary email; contact us to arrange a suitable method. If website features use cookies, analytics or external services that collect personal information, Estia will explain relevant collection and choices through the website or a collection notice.

Your rights and how to contact us

7. Provide access and correct information

You can ask for access to your personal information or request a correction by speaking with us, calling, emailing or writing to the Privacy Officer. We verify identity and any representative authority using reasonable checks. Access requests are acknowledged within 5 business days and responded to within 30 days. Agreed corrections are made within 7 days. We do not charge for making a request or correcting information; any reasonable access charge will be explained in advance.

If access or correction is refused where the law permits, we will explain the reasons in writing, unless we cannot lawfully do so, and explain complaint options. Where requested and required, we will attach a statement of a disputed correction to the record. We can help you make a request in your preferred communication format.

8. Respond fairly to privacy complaints

Contact the Privacy Officer if you believe information has been mishandled. You may have a supporter or advocate assist you. We acknowledge privacy complaints within 5 days, investigate fairly and aim to resolve them within 30 days. We explain the outcome and any corrective action. If more time is needed, we explain why and provide an update. Raising a concern will not affect your right to safe and respectful support.

Estia Privacy Officer - CEO / Company Secretary
Estia Foundation of Australia, 5-7 Pearson Street, Gladesville NSW 2111 Telephone: **02 9879 8000** | Email: **admin@estia.org.au**

If you are unhappy with our response, or do not receive a response within 30 days, you can complain to the **Office of the Australian Information Commissioner**: **1300 363 992** or www.oaic.gov.au/privacy/privacy-complaints. For NSW health information matters, you may also contact the **Information and Privacy Commission NSW**: **1800 472 679** or www.ipc.nsw.gov.au. Concerns about NDIS supports can be raised directly with the NDIS Commission on **1800 035 544**.

9. Act promptly on privacy breaches

Workers must immediately report suspected loss, unauthorised access or disclosure to the Privacy Officer. Estia will contain the breach, assess harm, take corrective action and review what happened. We take all reasonable steps to assess a suspected eligible data breach within 30 calendar days. Where notification is required under the Notifiable Data Breaches scheme, we notify the OAIC and affected individuals as soon as practicable, explaining the breach and protective steps.

Responsibilities and review

The Board oversees this policy. The CEO / Company Secretary acts as Privacy Officer and manages requests, complaints and breach responses. Managers ensure appropriate access and worker training; all workers must follow confidentiality requirements. This policy is available free of charge on our website and in an appropriate format on request. It is reviewed annually and following significant changes or privacy incidents.

Related requirements: Privacy Act 1988 (Cth) and Australian Privacy Principles; Health Records and Information Privacy Act 2002 (NSW); NDIS Code of Conduct and applicable NDIS Practice Standards.
Read with Estia's consent, information management, records retention, complaints and data breach response policies.