Integricare
Exceptional learning and care

CONFIDENTIALITY AND PRIVACY POLICY

SCOPE

This policy applies to all employees of Integricare.

RISK OBJECTIVE

To ensure that the confidentiality of information and files relating to the children, families, staff, and visitors using the Service is upheld at all times

POLICY PURPOSE

Integricare has an ethical and legal responsibility to protect the privacy and confidentiality of children, individuals and families as outlined in Early Childhood Code of Ethics, National Education and Care Regulations, and the Privacy Act 1988 (Cth) and subsequent amendments including the Privacy Amendment (Notifiable Data Breaches) Act 2017 and the Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022. The right to privacy of all children, their families, and educators and staff of the Service will be upheld and respected, whilst ensuring that all children have access to high quality early years care and education

DEFINITIONS

Prescribed Body

A prescribed body is any organisation specified in section 248(6) of the Act or in clause 8 of the Children and Young Persons (Care and Protection) Regulation 2012. Generally **prescribed bodies** are:

(a) State regulated education and care service within the meaning of the Children (Education and Care Services) Supplementary Provisions Act 2011,

(b) an education and care service within the meaning of the Children (Education and Care Services) National Law (NSW),

(c) a designated agency,

(d) a registered agency,

(e) an accredited adoption service provider within the meaning of the Adoption Act 2000,

(f) the Family Court of Australia,

(g) the Federal Magistrates Court of Australia,

(h) the Commonwealth Department of Human Services,

(i) the Commonwealth Department of Immigration and Citizenship,

(j) any other organisation the duties of which include direct responsibility for, or direct supervision of, the provision of health care, welfare, education, children's services, residential services, or law enforcement, wholly or partly to children.

Ref: https://legislation.nsw.gov.au/view/pdf/asmade/sl-2012-425

CONFIDENTIALITY AND PRIVACY POLICY

Social Media
Social media includes websites and other online means of communication that are used by large groups of people to share information and to develop social and professional contacts". Ref: Dictionary.com

Data Breach
A data breach is any unauthorised access to or disclosure of personal information, or loss of personal information that an organisation holds.

Notifiable Data Breach
A notifiable data breach is one that must be disclosed in accordance Part IIIC of the Privacy Act 1988.

Privacy Impact Assessment
A Privacy Impact Assessment is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimizing or eliminating that impact.

Privacy Officer
Privacy Officer means the designated staff member responsible for ensuring compliance with privacy laws and handling privacy-related inquiries, complaints, and breaches.

Integricare
Exceptional learning and care

CONFIDENTIALITY AND PRIVACY POLICY

GUIDING PRINCIPLES

Integricare aims to protect the privacy and confidentiality of all information and records about individual children, families, educators, staff, and management by ensuring continuous review and improvement of our current systems, storage, and methods of disposal of records.

We will ensure that all records and information are held in a secure place and are only retrieved by or released to people who have a legal right to access this information. Integricare takes data integrity very seriously, we strive to assure all records and data are protected from unauthorised access and that it is available to authorised persons when needed. This policy provides procedures to ensure data is stored, used, and accessed in accordance with relevant policies and procedures, for example, the enrolment policy, and CCS Account policy.

Under National Law, Section 263, Early Childhood Services are required to comply with Australian privacy law which includes the *Privacy Act 1988* (the Act) and all subsequent amendments aimed at protecting the privacy of individuals. Schedule 1 of the *Privacy Act* (1988) includes 13 Australian Privacy Principles (APPs) which all services are required to apply

THE POLICY PROCEDURE

Integricare will:

- ensure each Service acts in accordance with the requirements of the Australian Privacy Principles and *Privacy Act 1988* and all subsequent amendments by developing, reviewing, and implementing procedures and practices that identify:
    - the name and contact details of the Service;
    - what information the Service collects and the source of information;
    - why the information is collected;
    - who will have access to information;
    - collection, storage, use, disclosure, and disposal of personal information collected by the Service;
    - any law that requires the particular information to be collected;
    - adequate and appropriate storage for personal information collected by the Service;
    - protection of personal information from unauthorised access;
    - specific data retention periods for different categories of information in accordance with relevant legislation;
    - procedures for conducting Privacy Impact Assessments for new projects or significant changes to existing projects;
    - procedures for identifying, containing, assessing, notifying and reviewing data breaches in accordance with the Notifiable Data Breaches Scheme in Part III3 of the *Privacy Act 1988.*
- provide regular privacy training for all staff at least annually;
- ~~E~~nsure all relevant staff understand the requirements under Australia's privacy law and Notifiable Data Breaches (NDB) scheme;
- Maintain currency with the Australian Privacy Principles by designating a Privacy Officer responsible for overseeing all privacy-related activities and ensuring compliance;
- Ensure personal information is protected in accordance with our obligations under the *Privacy Act 1988* and *Privacy Amendments (Enhancing Privacy Protection) Act 2012* and *Privacy Amendment (Notifiable Data Breaches) Act 2017* and the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*;

CONFIDENTIALITY AND PRIVACY POLICY

- Ensure all records and documents are maintained and stored in accordance with relevant legislation; and
- Regularly back-up personal and sensitive data from computers to protect personal information collected;
- Ensure families are notified of the time particular records are required to be retained as per the relevant legislation;
- Ensure the appropriate and permitted use of images of children;
- Ensure all employees, students, volunteers, and families are provided with a copy of this policy;
- Provide families with a comprehensive Privacy Collection Notice at enrolment that clearly outlines what information is collected, why it is collected, how it will be used, and their rights regarding their information;
- Obtain specific consent for each distinct use of personal information beyond its primary purpose;
- Ensure families only have access to the files and records of their own children;
- Ensure the information given to Educators will be treated with respect and in a professional and confidential manner;
- Ensure individual child and staff files are stored in a locked and secure cabinet;
- Ensure information relating to staff employment will remain confidential and available on to the people directly involved with making personnel decisions;
- Ensure that information shared with a Service by families will be treated as confidential unless told otherwise;
- conduct regular privacy audits and security assessments of both physical and digital systems;
- Maintain a data breach response plan that is tested regularly.

Nominated Supervisors and/or Responsible Person will:

- adhere to Integricare's policies and procedures at all times;
- ensure Educators, staff, volunteers, and families are aware of the *Privacy and Confidentiality Policy;*
- ensure specific and written consent is gained from parents and/or guardians of children who will be photographed or videoed;
- ensure families only have access to the files and records of their own children;
- ensure that information given to Educators will be treated with respect and in a confidential and professional manner;
- ensure only necessary information regarding the children's day-to-day health and well-being is given to non-primary Educators, for example, food allergy information;
- ensure that information shared with us by the family will be treated as confidential unless told otherwise;
- immediately report any suspected or actual data breaches to the Privacy Officer;
- participate in regular privacy training.

Educators and staff will:

- read and adhere to the *Privacy and Confidentiality Policy* at all times;
- ensure documented information and photographs of children are kept secure but may be accessed at any time by the child's parents or guardian;

CONFIDENTIALITY AND PRIVACY POLICY

- ensure families only have access to the files and records of their own children;
- treat private and confidential information with respect in a professional manner;
- not discuss individual children with people other than the family of that child, except for the purposes of curriculum planning or group management. Communication in other settings must be approved by the family beforehand;
- ensure that information shared with the service by the family will be treated as confidential unless told otherwise;
- maintain individual and Service privacy of information and store documentation according to this policy at all times;
- not share information about individuals, services, management information, or other staff as per legislative authority;
- not share passwords or allow unauthorised access to systems containing personal information;
- immediately report any suspected or actual data breaches to their supervisor and the Privacy Officer; –

Management of confidential information:
Integricare is committed to protecting personal information in accordance with our obligations under the *Privacy Act 1988* and *Privacy Amendments (Enhancing Privacy Protection) Act 2012.*

Personal information includes a broad range of information, or an opinion, that could identify an individual. Sensitive information is personal information that includes information or an opinion about a range of personal information that has a higher level of privacy protection than other personal information. Source: OAIC-Australian Privacy Laws, Privacy Act 1988

Personal information will be collected and held securely and confidentially about you and your child to assist our Service provide quality education and care to your child whilst promoting and maintaining a child safe environment for all stakeholders

Method of Collection
Information is generally collected using standard forms at the time of enrolment or employment. Additional information may be provided to the Service through email, surveys, telephone calls or other written communication. Information may be collected online through the use of software such as CCS software or program software.

Where possible, we will collect personal information directly from the individual. When collecting personal information, we will take reasonable steps to notify the individual (or ensure they are aware) of certain matters, including the purposes for which we collect the information, the main consequence (if any) if they do not provide the information, and how they can access and correct the information.

How we protect your personal information
To protect your personal and sensitive information, we maintain physical, technical and administrative safeguards.

- All hard copies of information are stored in children's individual files or staff individual files in a locked cupboard.
- All computers used to store personal information are password protected.
- Each staff member will be provided with a unique username and password for access to CCS software and program software.

CONFIDENTIALITY AND PRIVACY POLICY

- Passwords must meet complexity requirements and be changed regularly.
- Staff will be advised not to share usernames and passwords.
- Access to personal and sensitive information is restricted to key personnel only.
- Security software is installed on all computers and updated automatically when patches are released
- Data is regularly backed up on an external drive and/or through a cloud storage solution
- Any notifiable breach of data is reported
- All staff are aware of the importance of confidentiality and maintaining the privacy and security of information.
- Procedures are in place to ensure information is communicated to intended recipients only, for example, invoices and payment inquiries
- Physical safeguards include secure areas for storage of physical records and secure disposal methods for confidential information.

Access to personal and sensitive information
Personal and sensitive information about staff, families, and children will be stored securely at all times. Families who have access to enrolment or program information online will be provided with a unique username and password. Families will be advised not to share usernames and passwords.

The Approved Provider will ensure that information kept in a child's record is not divulged or communicated through direct or indirect means to another person other than:

- The extent necessary for the education and care or medical treatment of the child to whom the information relates;
- A parent of the child to whom the information relates, except in the case of information kept in a staff record;
- The Regulatory Authority or an authorized officer;
- As expressly authorized, permitted or required to be given by or under any Act of law;
- Where required by a court order or subpoena;
- Where necessary to lessen or prevent a serious threat to an individual's life, health or safety, or public health or safety;
- With the written consent of the person who provided the information.

Personal Access
Clients and employees are able to access the information contained in their personal file, after a written or email request to the manager of a service, or in the case of employees, to the relevant senior manager.

Integricare is not required to give an individual access to personal information to the extent that:

1. Integricare reasonably believes that giving access would pose a serious threat to the life, health, or safety of any individual, or to public health or public safety;
2. giving access would have an unreasonable impact on the privacy of other individuals;
3. the request for access is frivolous or vexatious;
4. the information relates to existing or anticipated legal proceedings between Integricare and the individual, and would not be accessible by the process of discovery in those proceedings;
5. giving access would reveal the intentions of Integricare in relation to negotiations with the individual in such a way as to prejudice those negotiations;

6. giving access would be unlawful;
7. denying access is required or authorised by or under an Australian law or a court/tribunal order;
8. Integricare has reason to suspect that unlawful activity or misconduct of a serious nature that relates to Integricare's functions or activities has been/is being, or may be engaged in;
9. Giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
10. giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body;
11. giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Ref: Australian Privacy Principles12 March 2014 https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles

We will respond to requests for access to personal information within 30 days. If we refuse access, we will provide written reasons for the refusal and information about complaint mechanisms.

As children mature, we recognize their evolving capacity to make decisions about their personal information. We will consider the child's age, maturity, and understanding of the information when determining whether it is appropriate to provide access directly to the child or through their parent/guardian.

Disclosing personal and sensitive information

Integricare will only disclose personal or sensitive information:

- where required by law or a court/tribunal order;
- where necessary to lessen or prevent a serious threat to an individual's life, health or safety, or to public health or safety;
- where reasonably necessary for an enforcement related activity by an enforcement body;
- to a third-party provider with parent permission (e.g. CCS software provider, external agency involved in a professional relationship with the child);
- to a Child Protection Agency/Office of the Children's Guardian and Regulatory Authority as per our *Child Protection and Child Safe Policies*;
- as part of the purchase of our business asset with parental permission.

When a prescribed body requests information that relates to the safety, welfare or wellbeing of a particular unborn child, child, young person or class of children or young persons. *Children and Young Persons (Care and Protection) Act 1998 – Chapter 16A.* Before any exchange of information, the manager of a service must first discuss the request with a senior manager of Integricare.

In any such case, Integricare undertakes to advise the client wherever possible that the information has been requested or supplied in accordance with the above. In so doing, Integricare undertakes that any information so supplied will, so far as it can ensure, be treated in accordance with this policy.

Notifiable Data Breaches

Integricare recognises its obligations under the Notifiable Data Breach scheme. In the event of a data breach, we will:

1. Contain the breach and take immediate remedial action;
2. Assess whether the breach is likely to result in serious harm to affected individuals;
3. Notify affected individuals and the Office of the Australian Information Commissioner (OAIC) if a breach is likely to

result in serious harm;

4. Review the incident and take steps to prevent future breaches;

The Privacy Officer will lead the response to any suspected or actual data breach and maintain detailed records of all steps taken.

Data Retention
Integricare will retain personal information only for as long as it is required for the purposes for which it was collected or as required by law. Specific retention periods include:

- Children's records: Until the child reaches 25 years of age;
- Child assessments and program records: 3 years after the record was made;
- Incident, injury, trauma and illness records: Until the child reaches 25 years of ago;
- Medication records: 3 years after the child's last attendance;
- Financial records: 7 years.

Records will be destroyed securely when no longer required. Paper records containing personal information will be shredded, and electronic records will be permanently deleted.

Complaints
If a parent, employee or volunteer has a complaint or concern about our Service, or they believe there has been a data breach of the Australian Privacy Principles, they are requested to contact the ~~Approved Provider~~Privacy Officer so reasonable steps to investigate the complaint can be made and a response provided.
If there are further concerns about how the matter has been handled, please contact the Office of Australian Information Commissioner on 1300 363 992 or:

https://forms.business.gov.au/smartforms/landing.htm?formCode=APC_PC

Storage
Files remain the property of Integricare, not the employee or client. Integricare has the responsibility to ensure that files are stored securely. Staff should be aware that sensitive material is also recorded in staff diaries, appointment books and log books. These should be used in such a way as to maintain confidentiality.

Computers should be regarded as confidential records and all data stored regarding clients will be access coded with appropriate security levels in place. Disposal of confidential material should be conducted in such a manner as to preserve confidentiality, and client records should not be disposed of without authorisation from the CEO and in accordance with Integricare's Archiving policy (see below).

Agreement
All employees, on joining Integricare, will be informed about the privacy and confidentiality guidelines and sign the **FO15-01** *Privacy and Disclosure of Information Agreement* Form.

INTEGRICARE RELATED POLICIES AND PROCEDURES

Policies that are related to this policy and are to be read in conjunction with it are:

CONFIDENTIALITY AND PRIVACY POLICY

- **PC27** Confidentiality and privacy Policy
- **PO26** Child Protection Policy
- **Child Safe Policy**
- **PO06** Archiving Policy
- **PC12** Documentation Confidentiality and Security
- **PC03** Family Grievance Policy
- **PO22** Staff Grievance and Complaints Investigation Policy
- **PO32** Exchange of Information Policy

Forms that relate to this policy are **FO15** Privacy Disclosure of Information Agreement Form.

LEGISLATION

All employees of Integricare are required to abide by relevant authority regulations:

- Education and Care Services National Regulations 2011
- Children (Education and Care Services National Law Application) Act 2010
- Children and Young Persons (Care and Protection Act 1998
- Privacy Act 1988
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022
- Office of the Australian Information Commissioner. *Privacy fact sheet 17: Australian privacy principles.* January 2014.
- www.oaic.gov.au