POLICY:10.3 Confidentiality, Records and Register Management

Procedure: 10.5 Confidentiality and Privacy

The Service aims to ensure the privacy of all individuals is protected and all management personnel, Service staff and Educators are aware of their obligation to maintain confidentiality. The procedure links to 10.6 Record Management and Storage Procedure

10.5.1 Linking to Policy

This procedural guidance should be read in conjunction with the Service's **10.3 Confidentiality, Records and Register Management** and will assist the Approved Provider, management, staff (Nominated Supervisors, Coordinators and administrative staff members), Educators, Educator Assistants and parents to implement the policy. The procedure covers:

10.5.2 The National Privacy Principles (NPP)

The Service is committed to enacting the National Privacy Principles.

NPP 1: collection
Describes what an organisation should do when collecting personal information, including what they can collect, collecting from third parties and generally, what they should tell individuals about the collection.

NPP 2: use and disclosure
Outlines how organisations may use and disclose individuals' personal information. If certain conditions are met, an organisation does not always need an individual's consent to use and disclose personal information. There are rules about direct marketing.

NPPs 3 & 4: information quality and security
An organisation must take steps to ensure the personal information it holds is accurate and up-to-date and is kept secure from unauthorised use or access.

NPP 5: openness
An organisation must have a policy on how it manages personal information and make it available to anyone who asks for it.

NPP 6: access and correction
Gives individuals a general right of access to their personal information and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.

NPP 7: identifiers
Generally prevents an organisation from adopting an Australian Government identifier for an individual (e.g., Medicare numbers) as its own.

NPP 8: anonymity
Where possible, organisations must give individuals the opportunity to do business with them without the individual having to identify themselves.

NPP 9: transborder data flows
Outlines how organisations should protect the personal information that they transfer outside Australia.

NPP 10: sensitive information
Sensitive information includes information such as health, racial or ethnic background, or criminal record. Higher standards apply to the handling of sensitive information.

10.5.3 Managing Privacy and Confidentiality

The Service Staff and where applicable Educators will:

- only collect personal information so far as it relates to the service's activities and functions, and in line with relevant legislation. (National Privacy Principle 1.1 - Privacy Act 1998.)
- ensure the collection of personal information will be lawful, fair, reasonable, and unobtrusive. (National Privacy Principle 1.2 - Privacy Act 1998.)
- ensure individuals who provide personal information will be advised of:
    - The name and contact details of the service;
    - The fact that they can gain access to their information;
    - Why the information is collected; the organisations to which the information may be disclosed; any law that requires the particular information to be collected; and the main consequences for not providing the required information. (National Privacy Principle 1.3 – Privacy Act 1998).
- ensure the use or disclosure of personal information will only be for its original collected purpose unless the individual consents or unless it is needed to prevent a health threat or is required or authorised under law. (National Privacy Principle 2.1 – Privacy Act 1998).
- take steps to ensure the personal information collected, used or disclosed, is accurate, complete and up to date
- ensure personal information will be kept in a secure (locked or password protected draw or computer) and confidential way, and destroyed by shredding or incineration, when no longer needed. (National Privacy Principle 4 – Privacy Act 1998).
- ensure individuals will be provided with access to their personal information and may request that their information be updated or changed where it is not current or correct. (National Privacy Principle 6 – Privacy Act 1998).

- ensure individuals wishing to access their personal information are informed they must make written application to the Approved Provider or Nominated Supervisor who will arrange an appropriate time for this to occur, and;
- the Approved Provider/Nominated Supervisor will protect the security of the information by checking the identity of the applicant and ensuring someone is with them while they access the information to ensure the information is not changed or removed without the Approved Provider's/Nominated Supervisor's knowledge.

10.5.4 Roles and Responsibilities

The Approved Provider or Nominated Supervisor will:

- Deal with privacy complaints promptly and in a consistent manner and following the Service's Complaints Management Procedures. Where the aggrieved person is dissatisfied after going through the complaints process, they may appeal in writing to "The Director of Complaints, Office of the Federal Privacy Commission, GPO Box 5218, Sydney NSW 1042, or phone the Commissioner's Hotline on 1300 363 992. (Privacy Act 1998). www.privacy.gov.au or contact the Privacy Team, Office of the Information Commissioner, PO Box 10143, Adelaide Street, BRISBANE QLD 4001 Email: **administration@oic.qld.gov.au**
- Ensure all staff members and Educators are provided with explicit written guidelines detailing:
  - what information is to be kept confidential and why (see 10.6 Record Management and Storage Procedure for guidance)
  - what confidential information they may have access to fulfil their responsibilities and how this information may be accessed
  - who has a legal right to know what information
  - where and how confidential information should be stored. (see 10.6 Record Management and Storage Procedure for guidance).
- Ensure every enrolling parent/guardian is provided with clear information about:
  - what personal information is kept and why
  - any legal authority to collect personal information.
- third parties to whom the Service discloses such information as a usual practice.
- Ensure all personnel forms such as enrolment records, medical details and employee information will be stored securely. (Workplace Relations Act 1996).
- Ensure applicants, students or volunteers are informed that their personal information is being kept, for what reason, for how long, and how it will be destroyed at the end of the period.
- Ensure applicants are asked for their consent before their references are checked. Unsuccessful applicants are advised of when and how their personal information will be destroyed.
- Ensure all information about Educators will only be accessed by the Coordinator, Approved Provider and individual Educators concerned. (Workplace Relations Act 1996.)
- Ensure all matters discussed at Board and Committee Meetings will be treated as confidential (Privacy Act 1998.) unless otherwise stated.

Coordinators and Educators will ensure:

- Confidential conversations that Educators have with parents or the Coordinator has with Educators will be conducted in a quiet area away from children, as well as other parents and Educators. Such discussions are documented and stored in a confidential folder.
- They do not give information or evidence on matters relating to children and/or their families to anyone other than the responsible parent/guardian unless prior written approval by the responsible parent/guardian is obtained.
- Exceptions may apply regarding information about children when subpoenaed to appear before a court of law. Notwithstanding these requirements, confidential information may be exchanged in the normal course of work with other colleagues at the Service and may be given to the Approved Provider, when this is reasonably needed for the proper operation of the Service and the wellbeing of users and Educators. (Privacy Act 1988).
- Reports, notes and observations about children must be accurate and free from biased comments and negative labelling of children.
- Protect the privacy and confidentiality of other Educators by not relating personal information about another Educator to anyone either within or outside the Service.
- Students/people on work experience/volunteers will not make Educators, children or families at the Service an object for discussion outside of the Service (e.g., college, school, home etc.), nor will they at any time use family names in recorded or tutorial information.
- Students/people on work experience/volunteers will only use information gained from the Service upon receiving written approval from the Service to use and/or divulge such information and will never use or divulge the names of individuals.
- Discuss privacy and confidentiality with their families members and other residing at the residence where education and care is being provided to ensure they do not at anytime divulge private or confidential information about a child, their family or any other person involved at the Service.

Parents will:

- update their enrolment details annually, or whenever they experience a change in circumstances. Computer records will be updated as soon as new information is provided.

Review

	Date	**Details**
Revision 00	07/2015	Original Policy Issued
Revision 01	12/2016	Reviewed
Revision 02	08/2017	Reviewed
Revision 03	11/2020	Reviewed

Related Documents

Policies
10.3 Confidentiality, Records and Register Management

Reference
Refer to 10.3 Confidentiality, Records and Register Management