

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy	POD - PP	Governance Motion 9/19/7	People and Organisational Development (POD)	24/09/2019	01/09/2020 (Annually)

## PRIVACY POLICY (PP)

### 1 Purpose:

The purpose of this policy is to ensure the Glenfield Community Centre (“GCC”, “the Centre” including the Glenfield Early Learning Centre “GELC”) maintains privacy management practices that:

- a) Comply with the Privacy Act 1993, and the 12 Privacy Principles included therein;
- b) Promote a culture that protects and respects private information;
- c) Educate people within the Centre about information privacy; and
- d) Monitor privacy compliance and support the development of systems and processes that ensure privacy by design.

### 2 Scope:

This policy applies to all Centre staff, contractors and students.

This policy is not intended to be a stand-alone document. It must be read and applied in conjunction with:

- The Information Privacy Principles in the Privacy Act 1993;
- The agreements between the Centre and its Staff and Volunteers;
- The agreements between the GELC and its Students;
- The agreements between the Centre and its Contractors;
- Centre Privacy Statements; and
- All relevant law, including the Privacy Act 1993.

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy	POD - PP	Governance Motion 9/19/7	People and Organisational Development (POD)	24/09/2019	01/09/2020 (Annually)

### 3 Policy:

Policy statements are provided for each of the four desired outcomes as follows:

#### A) Comply with the Privacy Act 1993, including the 12 Privacy Principles:

##### 1 Collection of personal information (principles 1-4):

- 1.1. The Centre will collect personal information only where it is necessary to do so for a lawful purpose associated with normal Centre functions and activities, including where required to do so for reporting purposes.
- 1.2. The Centre will collect personal information directly from the individual concerned where it is practical and reasonable to do so unless an exception applies or unless the individual concerned consents otherwise.
- 1.3. The Centre collects information by various means and for a variety of purposes, and is required to be transparent about how, when and why it collects personal information. To achieve this transparency, the Centre will maintain and publish Privacy Statements that make people aware of the collection of their information, the purpose for doing so (including intended usage and disclosure), and the rights of individuals in respect to access and correction of their information.
- 1.4. The Privacy Statements will be published online at <https://gcc.net.nz/about-us/key-documents/policy/>, and/or linked to systems that collect and store personal information, such as: the GELC Student Enrolment System (Firstbase); Staff recruitment; and HR systems.
- 1.5. The Privacy Statements will be consistent at all times with this Policy, demonstrate good privacy management practice, will be maintained and fit-for-purpose at all times.
- 1.6. Collection, use and disclosure of personal information by the Centre (including people and processes and systems) must comply with the Privacy Statements.

<b>Policy:</b>	<b>Policy Manual No.</b>	<b>Authorised By:</b>	<b>Policy Section:</b>	<b>Effective:</b>	<b>Review Date:</b>
Privacy	POD - PP	Governance Motion 9/19/7	People and Organisational Development (POD)	24/09/2019	01/09/2020 (Annually)

## **2. Storage and security of personal information (Principle 5):**

- 2.1. Personal information, where classified as a record, will be retained and stored in accordance with the Information and Records Management Policy and Procedures and any requirements under statute.
- 2.2. Access to personal information, will be granted in accordance with the established approval processes for each system and/or data repository, and shall only be granted if required as part of a staff member's role.
- 2.3. Centre Staff must ensure personal information stored is protected from loss, misuse, or inappropriate disclosure, and maintain appropriate levels of access and system security, including ensuring that access to personal information is removed when no longer required by a role or individual.

## **3. Requests for access to and correction of personal information (Principles 6 and 7 plus parts 4 and 5 of the Act):**

- 3.1. The Centre acknowledges that unless an exception applies, individuals have the right to access their personal information, and the right to request correction of information.
- 3.2. Any GCC Governance or Staff member, Student (through their Parent/Caregiver/Guardian), member of the Public or their Agent may request access to personal information about themselves held by the Centre.
- 3.3. Where such a request is covered by an approved standard operating procedure and is a routine request, management receipt of the request should respond.
- 3.4. Non-routine requests, and those not covered by approved standard operating procedures must be reported to the Centre Manager and will be handled in accordance with the procedure outlined in the Guidelines for dealing with requests and corrections to personal information.

<b>Policy:</b>	<b>Policy Manual No.</b>	<b>Authorised By:</b>	<b>Policy Section:</b>	<b>Effective:</b>	<b>Review Date:</b>
Privacy	POD - PP	Governance Motion 9/19/7	People and Organisational Development (POD)	24/09/2019	01/09/2020 (Annually)

3.5. Anyone is entitled to request correction of their own personal information. Where such a request is made, the Centre must decide whether or not to correct the personal information. Once it has decided, the Centre must inform the requestor of its decision. If the Centre declines to amend the person's personal information, it must inform the person of their right to have their request and the Centre's refusal noted on their personal file. If a person decides to exercise this right, then the Centre must note the person's request and the Centre's refusal on the person's personal file.

#### **4. Accuracy of personal information (Principle 8):**

4.1. The Centre will take reasonable steps to ensure, prior to its use, that the information is correct, complete and up-to-date.

#### **5. Retention of personal information (Principle 9):**

5.1. Records containing personal information will be destroyed confidentially in accordance with the General Disposal Schedule (GDA), and the Centre's own procedures. Personal information collected that is not a Record requiring retention under the Public Records Act should be disposed of when it is no longer needed i.e. when the purpose for which it was collected has expired.

#### **6. Use and disclosure of personal information (Principles 10 and 11):**

6.1. The Centre will not disclose personal information for a purpose that is not consistent with that for which it was collected, unless required or permitted to do so by law, or consent has been obtained from individuals for their information to be disclosed for certain other purposes.

6.2. Centre staff must only access and/or use personal information where required to carry out a function of their employment with the Centre. In accordance with the Act, staff must also ensure:

- i) They do not disclose any personal (student or staff) information to another staff member, unless that staff member also has a professional need to use the information.

<b>Policy:</b>	<b>Policy Manual No.</b>	<b>Authorised By:</b>	<b>Policy Section:</b>	<b>Effective:</b>	<b>Review Date:</b>
Privacy	POD - PP	Governance Motion 9/19/7	People and Organisational Development (POD)	24/09/2019	01/09/2020 (Annually)

- ii) They do not disclose any personal (Governance, Staff or Student) information to another individual or organisation external to the Centre, unless authorised to do so.

## B) Promote a culture that protects and respects private information:

To promote and encourage a culture that protects and respects private information the Centre endeavours to model high standards of privacy practice and ensure that respect for the privacy of individuals is inherent in the operations of the Centre. Robust privacy practice will be ensured through the following:

### 1. Management of Privacy breaches:

All privacy breaches must be reported to the Centre Manager. A record of privacy breaches, and their remediation, will be maintained by the Centre Manager (or delegate). Privacy breaches must be remedied as soon as possible in consultation with the section where the breach occurred.

### 2. Responding to Privacy Complaints and investigations by the Privacy Commissioner:

All complaints received must be reported to the Centre Manager who may delegate the responsibility for investigation and management of the complaint. Complaints will be managed promptly and remedied as quickly as possible. Legal advice may be sought in respect of complaints that escalate to the Privacy Commissioner. Any complaint resulting in a settlement must be approved by Centre Governance.

### 3. All staff having a responsibility to:

- i) maintain good practice privacy behaviours;
- ii) report all privacy breaches to the Centre Manager who will act in the capacity as the Centre's "Privacy Officer";
- iii) understand and comply with obligations in regard to privacy, relevant to their position;
- iv) report and/or escalate concerns or issues relating to privacy; and
- v) ensure they are appropriately trained and/or informed of privacy handling practices relevant to their work.

<b>Policy:</b>	<b>Policy Manual No.</b>	<b>Authorised By:</b>	<b>Policy Section:</b>	<b>Effective:</b>	<b>Review Date:</b>
Privacy	POD - PP	Governance Motion 9/19/7	People and Organisational Development (POD)	24/09/2019	01/09/2020 (Annually)

**C) Educate people within the Centre about information privacy:**

An annual programme of awareness building and skills training will be provided to staff. The Privacy Policy and best practice privacy management practices adopted by the Centre, will be promoted to staff annually.

Staff managing systems must attend privacy training to ensure that their skill set and understanding is current and up-to-date. Staff operating and accessing such systems are strongly encouraged to attend privacy training or to complete an online privacy training module as part of their induction.

Systems that hold personal information shall incorporate aspects of best practice Privacy management into their training and induction materials, consistent with this Policy and the Centre's Privacy Statements.

**D) Monitor privacy compliance and support development of systems and processes that ensure privacy by design:**

Reports will be provided by the Centre Manager, or delegate, on progress against any specific privacy management work-plans, breaches and complaints, as required or requested.

Compliance with the Privacy Act 1993 will be reviewed in conjunction with the Policy Review Process each year, and all non-compliance will be reported.

Where systems containing personal information are planned, implemented, or significantly upgraded, a Privacy Impact Assessment must be undertaken including for any proposed developments where personal information is to be transferred overseas (including use of Cloud-based data information services).

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy	POD - PP	Governance Motion 9/19/7	People and Organisational Development (POD)	24/09/2019	01/09/2020 (Annually)

## 4 Definitions:

Terms not defined in this document may be in the **GCC Glossary of Terms**.

Terms and definitions:

- **Personal Information:** is any information, on its own or combined with other information, about an identifiable individual.

## 5 Legal Compliance:

- Privacy Act 1993
- Official Information Act 1982
- Health Information Privacy Code 1994
- Public Records Act 2005

This policy meets or exceeds current statute, bylaws or regulations.

## 6 Related Policy and Procedures:

- Information and Records Management Policies and Procedures

## 7 Document Management Control:

**Prepared by:** GCC Manager  
**Authorised by:** Governance Group  
**Approved by:** Governance Group Motion#: 9/17/9, 24 September 2019  
**Date issued:** September 2019  
**Last review:** September 2019  
**Next review:** September 2020  
**Effective Date:** September 2019