

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

## Privacy and Confidentiality Policy (PCP)

*Public-facing policy for collecting, using, storing, disclosing, protecting and responding to privacy and confidentiality matters*

Property of Glenfield Community Centre Incorporated

Last reviewed April 2026 | Next review April 2029 | Version 2026.1

### 1 Purpose:

The purpose of this policy is to ensure that Glenfield Community Centre Incorporated (GCC) collects, uses, stores, discloses, protects and disposes of personal information and confidential information in a lawful, respectful, transparent and secure manner.

### 2 Scope:

This policy applies to personal information and confidential information collected, held or used by GCC in relation to its Governance Group, officers, staff, volunteers, contractors, tenants, hirers, members, visitors, service users, website users, funders, suppliers, community partners and other stakeholders.

This policy applies to all Governance Group members, officers, staff, volunteers, contractors, advisers and any other person who collects, accesses, uses, stores, discloses, manages or disposes of personal information or confidential information on behalf of GCC.

This policy applies to information held in paper records, email, cloud systems, booking systems, accounting systems, employment records, membership records, complaint records, governance records, website forms, social media messages, photographs, images, video, security records and other digital or physical systems.

This policy does not replace specialist processes for employment records, protected disclosures, complaints, health and safety incidents, safeguarding, insurance claims, financial reporting, legal advice, funding accountability, or constitutional member records where a more specific legal or approved GCC process applies.

This policy must be read consistently with the GCC Constitution, including the Society's Principles, Objects, membership and member-register provisions, Governance Group powers, dispute-resolution requirements, financial-gain provisions and Appendix A values.

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

### 3 Policy Statement:

GCC respects the privacy, dignity and confidentiality of people who interact with the Centre. GCC will only collect personal information where it has a lawful and necessary purpose connected with its community, governance, employment, facility, room-hire, financial, funding, reporting, safety, membership or organisational activities.

GCC will be transparent about why it collects personal information, how the information may be used, who may receive it, how it is protected, and how people may request access to or correction of their information.

Personal information and confidential information must only be accessed, used or disclosed where there is a legitimate GCC purpose, appropriate authority, consent where required, or a lawful basis for doing so. Access must be limited to people who need the information to perform their role or support a lawful GCC function.

GCC will maintain reasonable safeguards to protect personal information and confidential information from loss, misuse, unauthorised access, unauthorised disclosure, alteration or destruction.

GCC will respond promptly and appropriately to privacy requests, privacy complaints and privacy breaches, including notifiable privacy breaches where a breach has caused, or is likely to cause, serious harm.

Confidentiality obligations continue after a person's employment, term of office, contract, volunteer role, tenancy, hire arrangement or other relationship with GCC ends.

### 4 Definitions:

**Personal Information:** Information about an identifiable individual, whether the information directly identifies them or could reasonably be combined with other information to identify them.

**Confidential Information:** Information that is not public and that GCC has a legitimate interest in protecting, including personal information, governance papers, financial information, employment records, complaints, contracts, security details, commercially sensitive information, passwords, access codes, unpublished plans and information entrusted to GCC by another person or organisation.

**Privacy Officer:** The person responsible for supporting GCC privacy compliance, privacy advice, privacy requests, privacy complaints and privacy breach management. For GCC, this role is performed by the Centre Manager unless Governance appoints another person.

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

**Privacy Breach:** Unauthorised or accidental access to, disclosure, alteration, loss or destruction of personal information, or an action that prevents GCC from accessing personal information on either a temporary or permanent basis.

**Notifiable Privacy Breach:** A privacy breach that has caused, or is likely to cause, serious harm to an affected individual and must be notified to the Office of the Privacy Commissioner and affected individual(s), unless an exception applies.

**Collection:** Obtaining, recording or receiving personal information from an individual or another source.

**Use:** Accessing, viewing, relying on, analysing, sharing internally or otherwise using personal information for a GCC purpose.

**Disclosure:** Sharing, releasing, publishing, showing or giving personal information to another person or organisation outside the people authorised to access it.

**Authorised Person:** A person who has a legitimate role-based need and authority to access, use or manage specific personal or confidential information.

**Privacy Request:** A request by an individual, or their authorised representative, to access or correct personal information held about them by GCC.

**Privacy Complaint:** A complaint that GCC has collected, used, stored, disclosed, retained or otherwise handled personal information in a way that may be inconsistent with this policy, the Privacy Act 2020, a privacy statement, or another relevant obligation.

**Representative:** A person authorised by an individual to support, assist or communicate on their behalf, such as a whānau member, advocate, legal adviser or community representative.

**Member Register:** The register of members required under the GCC Constitution and the Incorporated Societies Act 2022.

## 5 Roles and Responsibilities:

**Governance Group:** Approves this policy, maintains oversight of significant privacy and confidentiality risk, ensures privacy and confidentiality obligations are appropriately resourced, and receives reporting where matters raise governance, legal, financial, reputational, privacy, health and safety, employment, membership or systemic risk.

**Chair:** Ensures Governance-level privacy, confidentiality, conflict, complaint, member or officer matters are escalated and managed consistently with the Constitution and approved GCC policies.

**Centre Manager / Privacy Officer:** Owns implementation of this policy, acts as GCC Privacy Officer unless another person is appointed, manages or coordinates privacy requests, privacy complaints and privacy breaches, maintains privacy records, provides guidance to staff and Governance, and escalates significant matters to the Chair or Governance.

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

**Staff and volunteers:** Must protect personal and confidential information, collect only what is required, use information only for authorised GCC purposes, maintain secure records, report privacy or confidentiality concerns promptly, and follow approved systems and procedures.

**Contractors, tenants, hirers and service providers:** Must protect any personal or confidential information they receive through their relationship with GCC, comply with relevant agreements and privacy obligations, and cooperate with GCC where privacy or confidentiality issues arise.

**Governance Group members and officers:** Must use personal and confidential information only for proper governance purposes, protect meeting papers and records, manage conflicts of interest, and avoid unauthorised disclosure during or after their term of office.

**Individuals and representatives:** May request access to or correction of their own personal information and are expected to provide accurate information, keep GCC informed of relevant changes, and provide evidence of authority where acting through a representative.

## 6 Procedure / Implementation:

### 6.1 Collecting personal information:

GCC will collect personal information only where it is necessary for a lawful GCC purpose. This may include membership, governance, room hire, events, enquiries, complaints, employment, volunteering, contractor management, finance, payments, health and safety, reporting, funding, website communication, community engagement, security, and legal or regulatory compliance.

Where practicable, GCC will collect personal information directly from the individual concerned and will explain the purpose of collection, intended use, usual disclosures, whether collection is required or voluntary, and how the person may request access or correction.

### 6.2 Privacy notices, forms and consent:

GCC forms, agreements, booking processes, website forms, membership forms, employment documents and other information-collection points should include or link to an appropriate privacy statement where personal information is collected.

Consent should be clear, informed and proportionate where relied on. Where consent is not the basis for collection, use or disclosure, GCC must be able to identify another lawful basis.

### 6.3 Use and disclosure:

Personal information must only be used for the purpose for which it was collected, a directly related purpose, a purpose authorised by the individual, or another purpose permitted or required by law.

GCC will not disclose personal information outside GCC unless disclosure is authorised, necessary for a legitimate GCC purpose, required by law, required for health and safety, required for a funding, audit, insurance, regulatory or legal process, or otherwise permitted under the Privacy Act 2020.

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

#### 6.4 Storage, security and access control:

GCC will take reasonable steps to protect personal information and confidential information from loss, misuse, unauthorised access, unauthorised disclosure, alteration or destruction.

Security measures may include physical security, locked storage, role-based access, password protection, secure cloud or system permissions, secure disposal, limited sharing, audit trails where available, and removal of access when a person's role or relationship changes.

Personal and confidential information must not be stored on personal devices, personal email accounts or unapproved systems unless specifically authorised and appropriately protected.

#### 6.5 Accuracy, retention and disposal:

Before using personal information, GCC will take reasonable steps to ensure it is accurate, complete, relevant, up to date and not misleading for the purpose for which it is used.

Personal information and confidential information must be retained only for as long as required for the purpose for which it was collected, records-management requirements, legal obligations, financial or audit requirements, employment obligations, insurance, funding, dispute resolution, historical governance records or other legitimate GCC purposes.

Information no longer required must be securely disposed of, deleted, anonymised or archived in accordance with GCC records-management requirements.

#### 6.6 Access and correction requests:

Individuals may request access to personal information GCC holds about them and may request correction of that information. Requests may be made to the Centre Manager / Privacy Officer.

GCC will respond to privacy requests as soon as practicable and in accordance with the Privacy Act 2020. If GCC declines to correct information, the individual may ask for a statement of correction sought but not made to be attached to the information where required by law.

GCC may need to verify identity or authority before releasing information. Access may be refused or limited where a lawful ground applies, including where release would affect another person's privacy, breach confidence, prejudice legal processes, or create a safety or security risk.

#### 6.7 Member register and constitutional information:

GCC will manage the Member Register consistently with the GCC Constitution and applicable law. Member information must only be accessed by officers where necessary for the performance of their functions or exercise of their powers.

A member may request access to the Member Register through the Secretary. Access must be managed consistently with the Constitution, including the requirement that access is provided only to the extent members have consented to information about themselves being made available.

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

### 6.8 Confidential information:

Confidential information must only be used for legitimate GCC purposes and must not be used for personal advantage, unauthorised disclosure, unauthorised publication, or the advantage of another person or organisation.

People covered by this policy must not disclose confidential information during or after their relationship with GCC unless disclosure is authorised by GCC, required by law, required for a protected disclosure, required for health and safety, or otherwise lawful and appropriate.

When a person leaves a Governance, employment, volunteer, contractor, tenant, hirer or advisory role, they must return, delete or securely dispose of GCC confidential information, access credentials, keys, passes and records as directed by GCC.

### 6.9 Privacy breaches:

Any suspected or confirmed privacy breach must be reported immediately to the Centre Manager / Privacy Officer. Where the breach involves the Centre Manager, it must be reported to the Chair.

The Privacy Officer must contain the breach where possible, assess the nature and scale of the breach, consider the risk of serious harm, identify affected individuals, seek advice where required, record the breach, and decide whether notification is required.

If a breach is notifiable, GCC must notify the Office of the Privacy Commissioner and affected individual(s) as soon as practicable, unless an exception applies. Governance or the Chair must be advised of any notifiable breach and any significant privacy breach risk.

### 6.10 Privacy complaints:

Privacy complaints must be referred to the Centre Manager / Privacy Officer and managed in a way that is fair, timely, confidential and consistent with the Complaints and Feedback Policy where applicable.

GCC will generally seek to resolve privacy complaints directly with the person concerned. If the person remains dissatisfied, they may raise the matter with the Office of the Privacy Commissioner.

### 6.11 Website, online systems and cloud services:

GCC will maintain a Website Privacy Statement explaining how personal information may be collected through the website and online systems, including forms, analytics, email links, social media, embedded services or third-party platforms where applicable.

When adopting or materially changing systems that collect, store, process or transfer personal information, GCC must consider privacy risk, access controls, supplier reliability, overseas storage or disclosure, security arrangements, data retention and whether a Privacy Impact Assessment is required.

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

## 6.12 Training and privacy culture:

GCC will promote a culture that protects privacy and confidentiality. Staff, volunteers and Governance Group members must receive appropriate guidance, induction or training for the privacy and confidentiality responsibilities relevant to their role.

Privacy and confidentiality reminders should be included in relevant induction, employment, contractor, governance, complaint-handling, records-management, website and system-use processes.

## 7 Monitoring, Reporting and Breach Management:

GCC will maintain sufficient privacy records to support lawful management of privacy requests, privacy complaints, privacy breaches, access decisions, correction decisions, disclosure decisions, training, system changes and reporting.

The Centre Manager / Privacy Officer will report significant privacy or confidentiality matters, breach trends, notifiable breaches, systemic risks, training needs and recommended improvements to Governance at least annually, and sooner where risk requires.

Privacy breaches must be recorded whether or not they are notifiable. Records should include the date, nature of the breach, information affected, people affected, containment steps, harm assessment, notification decision, actions taken, advice received and closure date.

A failure to follow this policy may be managed through guidance, training, access removal, contract management, employment processes, Governance processes, membership processes, complaint management, legal advice, regulator notification or another lawful and proportionate action.

GCC will review this policy earlier than the scheduled review date if there is a significant privacy breach, complaint pattern, change in law, new system, technology change, audit finding, Governance direction or operational change affecting personal or confidential information.

## 8 Legal and Compliance Requirements:

This policy is intended to support compliance with current statutes, regulations, constitutional requirements, charitable obligations, funding obligations and recognised good-practice requirements relevant to privacy and confidentiality.

Relevant requirements include, but are not limited to:

- GCC Constitution;
- Privacy Act 2020;
- Incorporated Societies Act 2022;
- Charities Act 2005;
- Employment Relations Act 2000;

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

- Health and Safety at Work Act 2015;
- Human Rights Act 1993;
- Protected Disclosures (Protection of Whistleblowers) Act 2022;
- Unsolicited Electronic Messages Act 2007, where applicable;
- Auckland Council, Kaipātiki Local Board, lease, funding and accountability requirements; and
- recognised good-practice guidance relevant to privacy, records, cybersecurity, confidentiality and information management.

The Privacy Act 2020 includes 13 Information Privacy Principles covering collection, source, notice, manner of collection, storage and security, access, correction, accuracy, retention, use, disclosure, overseas disclosure and unique identifiers.

GCC must have at least one Privacy Officer. The Privacy Officer does not need to be a lawyer, but must be familiar with GCC's privacy obligations and able to support compliance.

The GCC Constitution prevails where it prescribes a process for the Member Register, member access, member complaints, Governance decision-making, financial gain, constitutional records or dispute resolution. If there is any inconsistency between this policy and the Constitution, the Constitution prevails unless Governance determines that the Constitution itself requires amendment to comply with law.

## 9 Related Documents:

- GCC Constitution;
- Policy and Procedure Framework;
- Master Policy and Procedure Register;
- Website Privacy Statement;
- Website Terms of Use;
- Complaints and Feedback Policy;
- Conflict of Interest Policy;
- Protected Disclosures Policy;
- Records and Information Management Policy, if adopted;
- Health and Safety Policy;
- Staff Code of Conduct;
- Governance Code of Conduct, if adopted;
- Employment policies and procedures;
- Room Hire Agreement and Room Booking Terms and Conditions;

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

- Membership forms and member records;
- Privacy Request and Complaint Register;
- Privacy Breach Register; and
- This policy supersedes the Confidentiality Policy (CoP) September 2019 and Privacy Policy (PP) September 2019 once approved.

## 10 Document Management Control:

<b>Prepared by</b>	Centre Manager
<b>Policy Owner</b>	Governance Group / Chair
<b>Authorised by</b>	Governance Group
<b>Approved by</b>	Governance Meeting Motion: [insert motion number]
<b>Date issued</b>	April 2026
<b>Last reviewed</b>	April 2026
<b>Review frequency</b>	Three-yearly, or earlier if legislation, governance, risk, funding, structure, privacy breach, system, technology or operational requirements change
<b>Next review</b>	April 2029
<b>Effective date</b>	[insert date approved]
<b>Version</b>	2026.1
<b>Visibility</b>	Public - Website
<b>Document ID</b>	GOV-PCP

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

## Appendix One - Examples of Personal and Confidential Information:

The following examples are indicative only. Information may still be personal or confidential even if it is not listed below.

Information type	Examples
Personal information	Names, contact details, membership records, booking contacts, payment information, complaint details, employment records, volunteer records, images, health and safety incident details, access requests, correspondence and any information about an identifiable individual.
Confidential governance information	Board papers, draft minutes, confidential meeting discussions, legal advice, disputes, proposed contracts, delegated decisions, conflicts of interest, strategic or financial matters not yet approved for release.
Confidential operational information	Passwords, alarm codes, keys, supplier details, contractor information, financial records, insurance matters, security arrangements, draft policies, internal procedures, tenant matters and unpublished plans.
Sensitive or higher-risk information	Information about complaints, employment, health, disability, safety, vulnerability, children, family circumstances, financial hardship, ethnicity, cultural identity, complaints, disputes or allegations of misconduct.

## Appendix Two - Privacy Request and Complaint Register Fields:

The Privacy Request and Complaint Register should record the following information where relevant, unless Governance approves a different structure.

Field	Purpose
Reference number	Unique request, complaint or breach reference.
Date received	Date the matter was received.
Person / representative	Name and contact details of the individual or authorised representative.
Type of matter	Access request, correction request, privacy complaint, confidentiality concern, disclosure request, or other privacy matter.
Information involved	Plain-English summary of the information or records involved.
System / location	Where the information is held, such as membership records, booking system, email, complaint file, employment file or finance system.
Action taken	Steps taken to verify identity, assess the request, gather information, respond or resolve the matter.

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

Field	Purpose
Decision / response	Access granted, correction made, request declined, statement attached, complaint resolved, referral made or other outcome.
Date closed	Date the matter was closed.
Follow-up required	System change, staff guidance, record correction, policy review, training, notification or other follow-up.
Privacy / confidentiality notes	Any access limits, withholding grounds, disclosure limits, affected third parties or special handling notes.

### Appendix Three - Privacy Breach Response Pathway:

The following pathway may be used as the basis for GCC privacy breach response and staff guidance.

Stage	Action	Indicative timeframe
Identify / report	Any suspected or confirmed privacy breach must be reported to the Centre Manager / Privacy Officer, or to the Chair if the matter involves the Centre Manager.	Immediately
Contain	Take reasonable steps to contain the breach, secure information, recover records, disable access, correct disclosure errors or prevent further loss.	As soon as practicable
Assess harm	Assess what happened, what information is affected, who is affected, whether serious harm has occurred or is likely, and whether specialist advice is required.	Urgently
Notify where required	If notifiable, notify the Office of the Privacy Commissioner and affected individual(s) as soon as practicable, unless an exception applies.	Ideally within 72 hours of becoming aware of a notifiable breach
Remedy and record	Record the breach, actions taken, advice received, notification decision, communication, remedial steps and closure date.	During response and at closure
Review and learn	Identify root cause, update systems, training, access controls, policies or procedures, and report significant matters to Governance.	At closure and during regular reporting

Policy:	Policy Manual No.	Authorised By:	Policy Section:	Effective:	Review Date:
Privacy and Confidentiality Policy (PCP)	GOV-PCP	Governance Group	Governance and Accountability (GOV)	Upon approval	April 2029; 3-yearly

## Appendix Four - Short Privacy Collection Statement Template:

The following wording may be adapted for GCC forms, online forms, membership documents, room hire documents or event registration where personal information is collected.

Scenario	Suggested wording
General collection statement	Glenfield Community Centre Incorporated collects the personal information you provide so we can respond to your enquiry, manage your booking, membership, event, complaint, payment, relationship with the Centre or other matter you have raised. We may use or disclose this information where necessary for those purposes, for legal or safety reasons, or as otherwise permitted by law. You may request access to or correction of your personal information by contacting the Centre Manager / Privacy Officer.
Complaint or incident statement	Information provided about a complaint, concern or incident will be used to assess, investigate, respond to, record and learn from the matter. We may need to share relevant information with people involved, Governance, advisers, insurers, regulators or other agencies where necessary and lawful.
Photography / media statement	Images or recordings that identify people will only be used where GCC has a lawful basis to do so, such as consent, event notice, legitimate community communication, or another lawful purpose. Additional care must be taken where children, vulnerable people or sensitive contexts are involved.