Confidentiality Policy (CoP)

Section	People and Organisational Development
Contact	GCC Manager
Last Review	June 2019
Next Review	June 2022
Approval	Governance Motion#: 6/19/3
Effective Date	June 2019
Version	1.0

Purpose:

The purpose of this policy is to explain how we expect our employees to treat confidential information relating to the Glenfield Community Centre Incorporated ("GCC", "the Centre").

Employees will unavoidably receive and handle personal and private information about clients and our organisation. We want to make sure that this information is well-protected.

We must protect this information for two reasons. It may:

- Be legally binding (e.g. sensitive customer data, employee personnel files.);
- Constitute the backbone of our business, giving us a competitive advantage (e.g. business processes.).

Scope:

This policy affects all employees, including Governance board members, contractors and volunteers, who may have access to confidential information. The term "Employee" will be used to refer to these groups collectively throughout this document.

Policy:

Employees must not disclose any information that is confidential to the Centre either during their employment or after termination of their employment. This disclosure includes disclosing confidential information to any other party. All organisational information must only be used for the purpose of work with the Centre.

Policy elements:

Confidential and proprietary information is secret, valuable, expensive and/or easily replicated. Common examples of confidential information are:

- Unpublished financial information;
- Data of Customers/Partners/Vendors;
- Patents, formulas or new technologies;
- Customer lists (existing and prospective);
- Data entrusted to our organisation by external parties;
- Pricing/marketing and other undisclosed strategies;
- Documents and processes explicitly marked as confidential;
- Unpublished goals, forecasts and initiatives marked as confidential.

Governance may have various levels of authorised access to confidential information.

When employees have any organisational information in their possession, they must take reasonable steps to safeguard the confidentiality of this information.

What employees should do:

- Lock or secure confidential information at all times;
- Shred confidential documents when they're no longer needed;
- Make sure they only view confidential information on secure devices;
- Only disclose information to other employees when it's necessary and authorised;
- Keep confidential documents inside the Centre's premises unless it's absolutely necessary to move them.

What employees shouldn't do:

- Use confidential information for any personal benefit or profit;
- Employees will not, at any time, without the Centre's approval, disclose or reveal any information to any other person or party whatsoever;
- Replicate confidential documents and files and store them on insecure devices.

On termination of employment, the employee shall immediately deliver to the Centre:

- All documents in his/her possession or power, including technical manuals, policy documents, and lists of clients and delete them from their personal devices;
- All copies or extracts from such documents in their possession;

- All keys and passes to the Centre or any related party of the Centre in their possession;
- Access passwords and login information for organisation email and websites.

Confidentiality Measures:

GCC will take measures to ensure that confidential information is well-protected.

We'll:

- Store and lock paper documents;
- Encrypt electronic information and safeguard databases;
- Ask employees to sign non-compete and/or non-disclosure agreements (NDAs) as required;
- Incorporate a statement relating to this policy in all employee contracts;
- Ask for authorisation by senior management to allow employees to access certain confidential information.

Exceptions:

Confidential information may occasionally have to be disclosed for legitimate reasons.

Examples are:

- If a regulatory body requests it as part of an investigation or audit;
- If our company examines a venture or partnership that requires disclosing some information (within legal boundaries);
- If an employee requests access to their own personnel file.

In such cases, employees involved should document their disclosure procedure and collect all needed authorisations. GCC is legally bound to avoid disclosing more information than needed.

Disciplinary Consequences:

Employees who don't respect our confidentiality policy will face disciplinary and, possibly, legal action.

We'll:

- Investigate every breach of this policy;
- Terminate any employee who wilfully or regularly breaches our confidentiality guidelines for personal profit. We may also have to punish any unintentional breach of this policy depending on its frequency and seriousness;

- Terminate employees who repeatedly disregard this policy, even when they do so unintentionally.

This policy is binding even after separation of employment.

Related Legislation:

Privacy Act 1993

Document Management Control:

Prepared by:	GCC Manager
Authorised by:	Governance Group
Approved by:	Governance Group Motion#: 6/19/3
Date issued:	June 2019
Last review:	June 2019
Next review:	June 2022
Effective Date:	June 2019