Gulf Harbour Marine Village Residents' Association

Privacy Policy

Table of Contents

Document Information

Document Name	Gulf Harbour Marine Village Residents Association Privacy Policy	
Document Owner	Gulf Harbour Marine Village Residents Association	
Approved by	Privacy Officer	Date: 18/02/26

Revision History

Version	Approved by	Description of changes

1. Purpose

A strong privacy culture is important to maintain the trust of our residents. We are committed to managing personal information held in accordance with our obligations under the Privacy Act and best practice.

2. Scope

This policy applies to all Committee Members, employees and contractors of GHMVRA. This policy also applies to all vendors who manage personal information on behalf of GHMVRA.

3. Definitions

Term	Definition
Personal Information	Any information which tells us something about a specific living individual. The information does not need to name the individual, as long as they are identified or identifiable in other ways, like through their movements, address or email address. Information about sole traders and companies can be considered personal information in some circumstances if it relates to an individual.
Privacy breach	An event where personal information is either inappropriately: • Disclosed • Altered • Lost - This includes either the destruction of information or inability to be able to access it. • Accessed.
Privacy Complaint	A complaint relating to the collection or handling of personal information including any notice, investigation or other action from the Office of the Privacy Commissioner.
Privacy Officer	The person(s) responsible for all privacy related matters at GHMVRA, monitoring compliance, acting as the contact for the Office of the Privacy Commissioner for breach notification, complaints and other enquiries and to ensure GHMVRA complies with the provisions of the Privacy Act.
Privacy Request	A request made by an individual to exercise any rights under the Privacy Act.
Vendor	A third party who completes actions on behalf of GHMVRA.

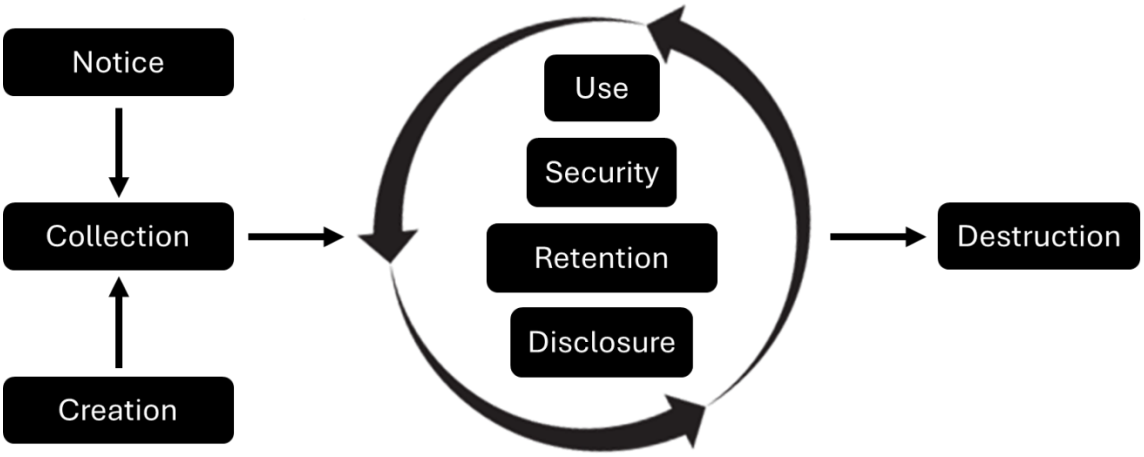
4. Overarching Principles

When managing personal information we are guided by the following overarching principles:

- We are a trusted guardian of personal information.
- We embody a culture in which personal information is protected and respected.
- All personal information is managed in line with the Privacy Act.

5. Information Lifecycle

All personal information must be managed throughout the entire information lifecycle from the point it is collected or created through to disposal.



5.1. Collection or Creation

When collecting information:

- Collect information directly from the individual concerned wherever possible and practicable.
- If information is collected from another organisation consider if they can legally provide it to us.
- Be balanced and not overly intrusive in how information is collected.

5.2. Notice

Individuals must be advised:

- What information is being collected and why.
- The purpose(s) for which their information will be used.
- Who the information may be shared with and why.
- How to access their information.
- How to complain about an interference with, or breaches of, their privacy.

Notice should be provided before personal information is collected in the form of a privacy statement.

5.3. Use

When using personal information, it must only be used for the purpose(s) it was collected for unless the individual authorises it. The purpose(s) are specified in the privacy statement provided at the time of collection.

Personal information should not be used in non-production environments.

Vendors must not use personal information for their own benefit e.g. creating statistical norms or adding email addresses to their own marketing lists.

5.4. Security

Safeguards must be in place to prevent, detect, recover from, and identify risk of loss from both internal and external systems. Controls must exist to prevent, detect, recover from, and identify risk of misuse both by staff and external parties.

Information must not be made available to people and organisations unless authorised.

5.5. Disclosure

Information held can only be disclosed where:

- Individuals were advised, in the privacy statement.
- There is a risk to public health or safety.
- It is required to enforce the law.
- Information about individuals is anonymised. Anonymising information is not just removing someone's name or contact information, instead anonymising information means making it so there is no way to re-identify the individual by combining pieces of information held.
- It is for statistical or research purposes.

5.6. Retention and Disposal

Information should be retained in accordance with the retention schedule. Information should be securely disposed when no longer required to be retained in accordance with the retention schedule.

Information held by vendors on behalf of GHMVRA must be disposed of when no longer required.

6. Training

Resources, training, and guidance material to support compliance with this policy will be made available by the Privacy Officer(s).

7. Privacy Assessments

Privacy Threshold Assessments (PTAs) are required to be completed for all new initiatives. New initiatives include:

- Undertaking a new project or initiative
- Implementing a new system or application
- Changing an existing initiative, system, guidance, and/or process / practice.

Privacy Impact Assessments (PIAs) are required to be completed for all high privacy risk initiatives, as determined by the Privacy Officer on completion of a PTA.

Privacy assessments (PTAs and PIAs) must be it must be signed off by a Privacy Officer before the process, policy or system is brought into effect.

8. Privacy Risk Management

Any identified privacy risks must be addressed in accordance with the risk management framework.

9. Vendor Management

Where we contract with a third-party vendor to outsource the processing of personal information you must ensure that the personal information is protected by equivalent safeguards to when it is managed by us.

Agreements must require the contracted party to meet our privacy requirements for example:

- Notify us of any privacy breach
- Notify us of any privacy act access or correction requests
- Maintain appropriate security safeguards
- Only retain information for a specified period
- Not sub-contract the processing to a lower standard than is agreed in the contract.

10. Privacy Breaches

All privacy incidents / breaches must be immediately contained. You must report any suspected privacy breach to the Privacy Officer(s). The Privacy Officer(s) will confirm whether there has been a privacy breach, and if it is notifiable.

Privacy breaches must be managed in accordance with the GHMVRA Breach Policy.

11. Privacy Requests

Privacy requests must be directed to the Privacy Officer(s). Requests must be handled as promptly as possible and responded to within at least 20 working days.

12. Privacy Complaints

Privacy complaints must be directed to the Privacy Officer(s). Complaints must be handled as promptly as possible and responded to within at least 20 working days.

13. Office of the Privacy Commissioner

Only the Privacy Officer(s) may communicate with the Office of the Privacy Commissioner unless otherwise authorised by the Privacy Officer(s). Any communications received from the Office of the Privacy Commissioner must be immediately provided to the Privacy Officer(s).

14. Roles and Responsibilities

Roles	Responsibilities
Committee Members	Each member of a committee is responsible for: • Ensuring that appropriate privacy systems, guidance, and practices to manage personal information. • Creating and nurturing a respectful privacy culture. • Ensuring systems and processes are in place to support effective identification and treatment of privacy risks (including privacy breaches).
Privacy Officer(s)	The Privacy Officer(s) are responsible for: • Reviewing compliance with applicable privacy legislation and good privacy practices. • Advising on identified privacy risks and proposed risk treatments. • Reviewing and approving privacy impact assessments for initiatives. • Providing advice and support GHMVRA on privacy matters. • Managing privacy breaches and complaints. • Communicating with the Office of the Privacy Commissioner. • Managing privacy requests from individuals.
All Staff including vendors	All staff and any staff of vendors who have contact with or manage personal information are responsible for: • Managing personal information in accordance with privacy systems, guidance, and practices (including any related contracts). • Identifying and raising privacy risks. • Reporting all privacy incidents / breaches.