



**Gulf Harbour Marine Village
Residents' Association
Privacy Breach Policy**

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Definitions	3
4. Privacy Breaches.....	4
4.1. What is a Privacy Breach?	4
4.2. Notifiable Privacy Breaches.....	4
5. Privacy Breach Process	5
5.1. Identifying the Breach.....	5
5.2. Containing the Breach	6
5.3. Assessing and Evaluating the Risk.....	6
5.4. Notification.....	6
5.5. Breach Learnings.....	7
6. Managing Breaches from Vendors.....	7
7. Managing the Media.....	7

Document Information

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

Revision History

Version	Approved by	Description of changes

1. Purpose

Privacy breaches are bad news. Loss or misuse of personal information can cause people harm and damage the trust of our residents.

It is therefore important that all Committee Members, employees and contractors of GHMVRA understand how to identify, record the required information and report potential privacy breaches so GHMVRA can respond appropriately and in a timely manner.

The following policy provides an overview of privacy breaches and the process GHMVRA follow when a breach is identified.

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 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.
Vendor	A third party who completes actions on behalf of GHMVRA.

4. Privacy Breaches

4.1. What is a Privacy Breach?

A 'Privacy Breach' occurs when personal information is inappropriately disclosed, altered, lost, or accessed. Loss includes either the destruction of information or the temporary inability to access information.

It doesn't change the fact of being a privacy breach if it:

- Was caused by a person inside or outside of GHMVRA
- Attributable in whole or in part to any action by GHMVRA
- Is ongoing.

'Inappropriately disclosed' or 'unauthorised disclosure' occurs when someone whether intentionally or unintentionally, make personal information accessible or visible to others outside the organisation, and release that information from our effective control in a way that is not permitted by the Privacy Act.

'Inappropriately accessed' or 'unauthorised access of personal information' occurs when personal information is accessed by someone who is not permitted to have access. This includes unauthorised access by GHMVRA users as well as unauthorised access by an external party (such as by hacking).

4.2. Notifiable Privacy Breaches

New Zealand's Privacy Act 2020 requires privacy breaches that have or may cause 'serious harm' to the individuals affected to be reported both to the Office of the Privacy Commissioner (OPC) and normally to the affected individuals themselves "as soon as practicable". Guidance from the OPC states this should be within 72 hours. These types of breaches are called notifiable privacy breaches.

Without reporting privacy breaches as soon as they are identified or suspected, GHMVRA may not be able to fulfil its legal obligations under the Privacy Act 2020.

Serious harm can include:

- Specific damage (such as physical injury)
- Loss of a benefit (such as lost income) or
- Emotional harm (such as significant humiliation, loss of dignity or hurt feelings).

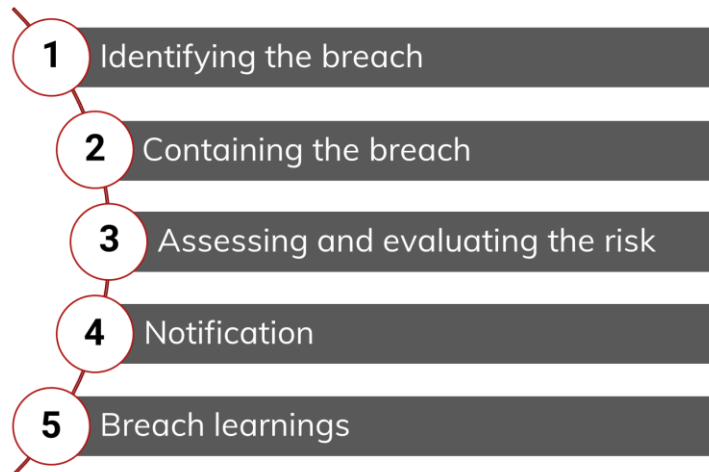
Whether harm is serious harm depends on the unique circumstances of each breach therefore each breach needs to be uniquely considered to determine if the breach has or is likely to have caused serious harm to the affected individuals.

GHMVRA's Privacy Officer(s) are responsible for the assessment of harm and determining if serious harm has or may occur.

5. Privacy Breach Process

The privacy breach process must be used in the event of a privacy breach, or where a privacy breach is suspected.

There are five basic steps to the Privacy Breach Process:



5.1. Identifying the Breach

The first step in the process is to determine if a privacy breach has occurred, how the breach has come about and if and what personal information was involved. The key is to gather enough information to then make an initial judgement call and to inform the correct people within GHMVRA.

As part of the identification step, it should be determined:

- What personal information may have been involved
- The cause of the breach
- How the breach was discovered
- Who is aware of the incident

Any GHMVRA Committee Members, employees or contractors who discover or is notified of a suspected or actual privacy breach must immediately report it to GHMVRA's Privacy Officer(s). The Privacy Officer will work with confirm the details of the breach and confirm whether they believe a breach has occurred.

GHMVRA maintains a log of all privacy breaches and near misses. This log will include the details of the breach, its effects and the remedial actions taken. It is the Privacy Officer's responsibility to maintain this.

The Police will be informed by the Privacy Officer(s) if the breach involves theft or other criminal activity.

5.2. Containing the Breach

Once a privacy breach (or suspected breach) has been identified and confirmed the first thing is take steps to stop the privacy breach getting worse. As time is of the essence containment should commence even before having informed relevant parties.

The Privacy Officer will advise on actions to be taken.

5.3. Assessing and Evaluating the Risk

During this step of the Privacy Breach Process the Privacy Officer(s) gather the facts and evaluate the risks, including assessing the potential harm to affected individuals and the risk of the breach reoccurring.

The assessment should start as soon as containment has been achieved. The Privacy Officer will assess the risks of the privacy breach to help determine the next steps and importantly whether the breach is notifiable or not. The Privacy Officer will use the Privacy Commissioner Notify Us tool to guide if it is notifiable.

5.4. Notification

A privacy breach is 'notifiable' if it has caused or is likely to cause, serious harm to any individual involved in the privacy breach. The Privacy Officer(s) is accountable for confirming on a case-by-case basis whether a breach is a notifiable privacy breach.

GHMVRA is legally required to notify OPC of any notifiable privacy breaches as soon as reasonably practicable, within 72 hours. All privacy breaches must be notified via OPC's online notification tool NotifyUs. The Privacy Officer(s) are responsible for informing OPC of all notifiable privacy breaches.

Where a privacy breach is notifiable GHMVRA must also notify the individuals affected

The notification to the individual must include:

- A description of the breach
- The steps GHMVRA plan to take regarding the breach
- The steps an individual could take to mitigate or avoid potential loss or harm
- Confirmation that the OPC has been notified
- That the individual has the right to make a complaint to the OPC
- Contact details for the Privacy Officer.

A privacy breach does not need to be 'notifiable' for the Privacy Officer to decide that it is best for the affected individuals to be informed. This is also a case-by-case decision based on the relevant benefit of contacting people against any harm notifying people could cause.

5.5. Breach Learnings

Privacy breaches provide a learning opportunity for GMVRA. It is important that all privacy breaches are reviewed for any important lessons.

6.Managing Breaches from Vendors

Should a breach involve a vendor holding information on behalf of GHMVRA then the same privacy breach process should be followed as per any other breach. The contractual relationship with the vendor may include provisions requiring them to assist GHMVRA so these should be reviewed.

7.Managing the Media

There may sometimes be media interest in a privacy breach. If GHMVRA receive a request from the media, then the breach must be immediately escalated to the Privacy Officer(s).