Privacy Policy and Guideline Manual

Whiddon

Document Control

Title	Privacy Policy and Guidelines
Version	**7.0**
Effective Date	August 2023
Review Date	December 2024
Initiating service area	Compliance and Risk
Release Authority	CEO

Document Review

Date	Description of review	Initiated by	Version
14/05/2015	Added in entries regarding storage of digital information	Regan Stathers	1.0
2/03/2018	Privacy Amendment (Notifiable Data Breaches) Act 2017; Data Breach Response Plan	Wake GMC&R	1.1
Feb 2019	Single Quality Framework review, Branding, Inclusion of surveillance in policy	Wake GMC&R	2.0
18/04/2019	Policy published	Wake GMC&R	2.1
26/06/2019	Policy/ Data Breach and Privacy Manual Combined into the one document. Manual updated – Overview table added. Open disclosure in complaints method referenced. Executive administration added as contact for correspondence. Consent for use of information and Privacy brochure updated. MyLearning module Privacy in the Workplace added. Employee Obligations added / Privacy agreement	Wake GMC&R	3.0
29/07/19	Review - Legal/78140688_4 Thomson Geer	Wake GMC&R	4.0
03/09/19	Feedback from CG incorporated. Changes to Open disclosure language.	Wake GMC&R	4.1
22.3.21	Review considering Whiddon roles, update of links to documents on OAIC. Inclusion of COO in IMT if breach occurs	Wake GMC&R	5.0
March 22	Review considering digital visitor screening and ongoing trials + changes using modern CCTV platforms.	Stathers EGMT&P	6.0
May --August 2023	Review by Thomson and Geer and Henein Nader Separate Policy, Manual from NDB response plan. Review of NDB to reflect OAIC guide	Wake Stathers Jarrett	**7.0**

Contents

Policy Overview

The *Privacy Act 1988* (Privacy Act) regulates the way individuals' personal information is handled.

As an individual, the Privacy Act gives a person greater control over the way that their personal information is handled. The Privacy Act allows residents and clients to:

- Know why their personal information is being collected, how it will be used and to whom it will be disclosed.
- Be anonymous, or of use a pseudonym in certain circumstances.
- Ask for access to their personal information (including their health information).
- Stop receiving unwanted direct marketing.
- Ask for their personal information that is incorrect to be corrected.
- Complain if they believe that Whiddon has mishandled their personal information.

Legislation that entity is governed by	Aged Care Act 1997 (Cwlth) Aged Care Accreditation Standards
Guiding Regulations	• Privacy Act 1988 (Cwlth) • Australian Privacy Principles • Privacy Regulation 2013 • Health Records and Information Privacy Act 2002 (NSW) • Health Records and Information Privacy Regulation 2017 • Health Privacy Principles • My Health Records Act 2012 (Cwlth) • My Health Records Rule 2016 (Cwlth) • My Health Records Regulation 2012 (Cwlth) • Spam Act 2003 (Cwlth)

Privacy

Introduction

Whiddon is a not-for-profit entity that provides care services including nursing, respite, residential and in-home care services throughout New South Wales and Queensland.

Whiddon is committed to ensuring that the personal information that we collect and hold about individuals is safeguarded and protected. We are also open and transparent about the way we collect and use this personal information.

The Australian Privacy Principles (APPs), which are contained in schedule 1 of the Privacy Act 1988 (Privacy Act), outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information.

This privacy policy (Policy) sets out information about how Whiddon meets its obligations under the Privacy Act, including the APPs, and the Personal Information that Whiddon collects and uses. The policy also sets out the rights of an individual in relation to privacy and the steps that Whiddon takes if a breach of privacy occurs.

Application of Policy

This Policy extends to all operations and functions of Whiddon, it covers the collection, handling, use and disclosure of personal information.

Personal information held by Whiddon, relating to current or former employment, isn't covered by the Australian Privacy Principles, but only when used by Whiddon directly in relation to their employment. (Fair Work Commission; Tools and Resources – Best Practice Guide / Rules about employee's personal information) This information includes:

- The employee's personal and emergency contact details
- Information about terms and conditions of employment
- Wage or salary details
- Leave balances.
- Records of work hours
- Records of engagement, resignation, or termination of employment
- Information about training, performance, and conduct
- Taxation, banking, or superannuation details
- Union, professional or trade association membership information.

The Australian Privacy Principles do apply to personal information about unsuccessful job candidates. This can include applicants' resumes, contact details, references, and academic transcripts.

Definitions

Personal information[1] is information or an opinion about an identified individual, or an individual who is reasonably identifiable,

- Whether the information or opinion is true or not; and
- Whether the information or opinion is recorded in a material form or not

Reasonably identifiable means whether an individual is 'reasonably identifiable' from information will depend on considerations that include: [2]•

- The nature and amount of information
- The circumstances of its receipt
- Who will have access to the information?
- Other information either held by or available to the APP entity that holds the information.
- Whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable.
- If the information is publicly released, whether a reasonable member of the public who accesses that information would be able to identify the individual.

A sub-category of Personal Information is sensitive information.

Sensitive information[3] includes information of a particularly sensitive nature, including.

- An individual's health information,
- Genetic information,
- Biometric information,
- Biometric templates,
- Racial or ethnic origin,
- Political opinions,
- Membership of a trade union or political association,
- Religious beliefs or affiliations,
- Philosophical beliefs,
- Sexual identity or,
- Criminal record

[1] OAIC Australian Privacy Principles Guidelines, B.88

[2] OAIC Australian Privacy Principles Guidelines, B.94

[3] OAIC Australian Privacy Principles Guidelines, B.141

- Health information about an individual
- Genetic information (that is not otherwise health information)
- Biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- Biometric templates

Health information[4] is Health information is any personal information about your health or disability. It includes information or opinion about a person's illness, injury, or disability.

Some examples of health information include:

- Notes of your symptoms or diagnosis
- Information about a health service you've had or will receive.
- Specialist reports and test results
- Prescriptions and other pharmaceutical purchases
- Dental records
- Your genetic information
- Your wishes about future health services
- Your wishes about potential organ donation
- Appointment and billing details
- Any other personal information about you when a health service provider collects it.

As a provider of aged care services, Whiddon collects a significant amount of Sensitive Information, including clients' medical records, test results and medications.

Policy statement

Whiddon respects individual's rights to privacy and personal information is kept confidential.

Whiddon ensures that the management of personal information is open and transparent and includes having a clearly expressed and up to date privacy policy (this policy).

Whiddon is guided by the Australian Privacy Principles (APPs) in its approach to privacy and personal sensitive information and:

- Is open and transparent in its management of personal information.
- Facilitates individuals having the option of transacting anonymously or using a pseudonym where practicable.

[4] OAIC – Privacy - What is health information? website.

- Gives notice to individuals whenever personal information is collected and how personal information may be used and disclosed and provides a mechanism for correction of personal information.
- Ensures the quality of personal information is maintained, accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.
- Keeps personal information secure and protects personal information from misuse, interference, and loss, and from unauthorised access with supportive operational and technological systems.

Your Privacy Rights

Privacy is acknowledged as a fundamental human right. In Australia, the *Privacy Act 1988* deals with your information privacy rights and how organisations and agencies must handle your personal information.

Australian privacy law gives individuals a general right to access their personal information. This includes health information. Whiddon provides access to personal information when it is requested by an individual or their authorised representative. There is no right under Australian privacy law to access other kinds of information, such as commercial information.[5]

- Whiddon provides access for individuals to their information and correction of their personal information.
- Whiddon does not use government related identifiers as identifiers in Whiddon specific systems.
- Whiddon practises Open Disclosure in relation to complaints, incidents, errors, and near misses.
- Whiddon complies with notification requirements if a data breach occurs.

[5] OAIC Accessing personal information.

Whiddon Privacy Policy

The Frank Whiddon Masonic Homes of NSW (trading as Whiddon) is a not-for-profit entity (**Whiddon, we, our** and **us**) that provides care services including nursing, respite, residential and in-home care services throughout New South Wales and Queensland. This Privacy Policy outlines how we will handle personal information under the applicable privacy laws.

Personal information is any sort of information or an opinion about an individual which identifies that individual, or which can be used to identify them. Personal information includes health information and other sensitive information like genetic information, biometric information, biometric templates, and information about the individual's racial or ethnic origin, political opinions, membership of a trade union or political association, religious beliefs or affiliations, philosophical beliefs, sexual preferences, or criminal record.

Please note that in some circumstances, there are exemptions or exceptions to the privacy laws that may apply to Whiddon, including in relation to the handling of employment related personal information. Nothing in this Privacy Policy is intended to limit the operation of those exemptions or exceptions to Whiddon or to otherwise restrict us from collecting and handling personal information in a manner that would otherwise be permitted by law.

Whiddon complies with the Notifiable Data Breach (NDB) scheme and will notify affected individuals and the Australian Information Commissioner (Commissioner), in the event of an eligible data breach.

This policy outlines:

- What data we collect; the kinds of personal information collected and held by Whiddon.
- We collect personal, health and sensitive information.
- How personal information is collected and held.
- We collect information directly from residents, clients and their representatives and other services providers involved in the care of the consumer, visitors, contractors, and staff.
- Personal, sensitive and health information is stored in password protected software systems designed for purpose or if in hard copy designated secure document storage areas.
- What we do with this data; the purposes for which personal information is collected, held, used, and disclosed
- We use this information in relation to care services including nursing, respite, residential and in-home care services throughout New South Wales and Queensland and associated business operations and employment.
- To contact you regarding providing care services including nursing, respite, residential and in-home care services throughout New South Wales and Queensland and associated business operations and employment
- Who we share information with

- We share this information with other authorised entities (authorised by us or the Department of Health and Aged Care) to provide care services including nursing, respite, residential and in-home care services throughout New South Wales and Queensland and associated business operations and employment.
- Collection of personal data by — and the disclosure to — governmental institutions and authorities will be carried out only based on specific legal provisions. In all cases, this privacy policy imposes those restrictions that are necessary to meet the legal requirements of the respective laws.
- We do not send information overseas, if software vendors are based overseas, they comply with Australian Privacy Laws.
- Your rights
- You have the right to access and or correct personal information that Whiddon has collected about and from you.
- Who to contact if you have questions or complaints.

Questions or complaints may be sent to

Frank Whiddon Masonic Homes of NSW
Attn: Support Services - Executive Administration Team
Locked Bag 7014
Minto NSW 2566
execadmin@whiddon.com.au.

A request for access to an individual's information must be in writing addressed to:

Frank Whiddon Masonic Homes of NSW
Attn: Support Services - Executive Administration Team
Locked Bag 7014
Minto NSW 2566
execadmin@whiddon.com.au.

Management of Electronic Data

Whiddon's web servers automatically record the Internet Protocol (IP) addresses of visitors. The IP address is a unique number assigned to every computer on the internet. Generally, an IP address changes each time you connect to the internet (it is a "dynamic" address). Note, however, that if you have a broadband connection, depending on your individual circumstance, the IP address that we collect may contain information that could be deemed identifiable. This is because, with some broadband connections, your IP address doesn't change (it is "static") and could be associated with your personal computer.

Whiddon servers also capture and store information that your browser transmits. This includes:

- Browser type/version/plug-ins used or security levels.
- Operating system used.
- Media Access Control (MAC) address

- Screen resolution
- Date and time of the server request
- Location-related data (such as the geographic location of the IP address)
- Volume of data transferred.
- Access status (“file transferred,” “file not found” and so on)

We will not deduce personal information from this data.

By using our website at www.whiddon.com.au and/or providing us with your personal information, you consent to us handling your personal information in accordance with this Privacy Policy.

If you choose to contact Whiddon staff using an email address, a discussion forum, a blog, a text message, or other electronic communication method, or if you choose to complete an online form provided on the Whiddon website (e.g., a customer feedback form), we may ask you to provide your name, email address or other personal data. You will be provided with a notice of collection statement, which includes Whiddon’s legal authority for the collection; the principal purposes for which the personal data is intended to be used; and the title, business address and business telephone number of a Whiddon employee who can answer questions about the collection.

Why Do We Collect This Information

The purpose of collecting this information is to allow staff to respond to your inquiry or to evaluate individual web services. Only authorized staff will have access to the information provided, and the information will be used only for the purpose it was intended. Completed surveys are sent to staff anonymously. We will ask you to provide us only with a method of contacting you (email, phone, fax or mailing address) if you wish to be included in future surveys or to have us respond to you.

From time to time, we record phone calls for training purposes. If you do not wish your call to be recorded, please inform the person you are calling or the operator or hang up.

How Do We Protect Personal Information

Whiddon implements commercially reasonable technical and organizational security controls to protect collected personal data against theft, loss, or misuse. Data is stored in a secure operating environment that is not accessible without authorisation. Whiddon applies mitigation measures following periodic risk assessments to ensure an adequate level of protection of personal data.

Please note for business continuity and disaster recovery purposes, Whiddon may store data in a location outside the jurisdiction(s) in which we normally operate. In such scenarios, we will implement all commercially reasonable measures to protect personal data against theft, loss, or misuse.

Whiddon does not knowingly collect data from or about children under 16. If we learn that we have collected personal information from a child under 16 we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under 16 please contact us at **execadmin@whiddon.com.au**

To maximize privacy protection, Whiddon structurally deletes your personal information after the useful period. Following legal requirements:

- **To manage the service —** We retain the personal data as indicated for this purpose for 7 years.
- **To contact you —** We retain the personal data as indicated for this purpose for 7 years after the care or employment relationship has ended to ensure regulatory requirements are met.

Access to this Policy

This Policy can be accessed via Whiddon's website www.whiddon.com.au. Individuals can also request a free copy of the policy direct from Whiddon, in which case it must be provided to the requesting individual in a timely manner.

Changes to this Policy

The policy is reviewed in accordance with Policy review schedules, continuous improvement, and regulatory changes. Details of reviews can be found in the 'Document Review' section of this document.

Recommendations for change to this policy should be sent to the Deputy Chief Executive Officer by email.

Whiddon's Privacy Guideline Manual

Purpose of this Guideline

Whiddon is committed to ensuring that the personal information that we collect, and hold is safeguarded and protected. We are also open and transparent about the way we collect and use personal information.

This Manual outlines the obligations of all Whiddon's directors, management, employees, volunteers, contractors and agents (**Personnel**) to ensure that we comply with the Privacy Act 1988, and the Australian Privacy Principles (APPs) and the ***My Health Records Act 2012*** (My Health Records Act), and ***My Health Records Regulation 2012*** which create the legislative framework for the Australian Government's My Health Record system. The My Health Records Act limits when and how health information included in a My Health Record can be collected, used, and disclosed. Unauthorised collection, use or disclosure of My Health Record information is both a breach of the My Health Records Act and an interference with privacy.

All Personnel must familiarise themselves with this Manual. If there is any aspect of this Manual that you do not understand or would like to clarify, you should raise this with your manager.

Scope of this Manual

This Manual extends to all operations and functions of Whiddon, excluding employee records.

This Manual outlines obligations under the Whiddon Privacy Policy. In the event of any inconsistency between this Manual and the Privacy Policy, the content of the Privacy Policy takes prevalence.

The Manual covers the collection, handling, use and disclosure of personal information, including sensitive information.

Training

Employees and volunteers are required to complete the MyLearning module: Privacy and the Workplace.

The course provides the learner with an understanding of the right to privacy and how personal information must be protected.

Personnel obligations and non-compliance

Employees, contractors, and volunteers are required to abide by the Whiddon Code of Conduct which outlines expectations in relation to privacy.

Employees and volunteers are required to sign a Privacy Agreement which outlines their obligations in relation to privacy. Further detail is provided in the employee and volunteer handbooks.

Performance management procedures may be initiated for breaches of the Privacy Agreement.

Further, all Whiddon Personnel are responsible for ensuring that they understand and comply with this Manual and the procedures implemented by Whiddon in relation to privacy and data protection. Failure to comply with this Manual may result in disciplinary action, which may include potential termination of employment or contract of engagement.

Collecting Personal Information

Only personal information that is relevant and directly related to the provision of services to our clients or to our business functions and activities may be collected.

Before Personal Information is collected from an individual they must be provided with a copy of Whiddon's Privacy Brochure and, in the case of residents or clients, has signed the Client Consent form for use of information.

Once the client has signed the Client Consent Form personal information may be collected from any of the following persons:

- The client's medical, nursing and care providers.
- Whiddon's contractors and agents such as pathology and X-Ray services, pharmacies, and hospitals; and/or
- A person nominated by the client on the client's Consent Form or otherwise expressly nominated by the client.

In some circumstances, if a client or resident lacks capacity (for example, because of their age or mental capacity) personal information may be collected from their authorised representative. Please note that the client's authorised representative must be either:

- An attorney for the individual under an enduring power of attorney in relation to health care.
- A guardian or person responsible under the Guardianship Act 1987; or
- A person with power at law to act as a representative of the individual (Authorised Representative)

Never assume that a next of kin or a relative is the client's authorised representative or has been nominated by the client. It is important to verify who a client's authorised representative is and who the client has nominated against the client's file.

Occasionally, Whiddon may receive unsolicited Personal Information relating to our clients, volunteers, applicants, contractors, and agents. Unsolicited information is information that has not been solicited or requested by us. An example of unsolicited personal information is information that a third party might provide to us about a client's alleged personal affairs.

Whiddon must not retain unsolicited Personal Information unless the information could have been collected under the above collection process, including that it is the type of personal information that Whiddon is permitted to collect, and the personal information is collected from a person with authority to provide that information.

You must advise your manager if you receive unsolicited Personal Information. Your manager will then verify that it is unsolicited Personal Information that should be permanently and securely destroyed. If it is not possible to destroy the information, the information must be de-identified.

Anonymity and pseudonymity

Under Australian privacy law individuals have the right to request that we deal with them on an anonymous basis unless it is not legal, or it is impracticable for us to do so.

Given the nature of the services that Whiddon provides in most circumstances it will not be practicable for individuals, especially current clients, to deal with us on an anonymous basis or using a pseudonym. However, an individual may make a written request to deal with us anonymously or using a pseudonym. A request may be granted based on the circumstances of the case.

An example of a situation where we might permit an individual to deal with us anonymously is where he or she is making an enquiry about our services or volunteering opportunities.

Protecting personal information

At all times you must protect the Personal Information that we hold, whether that information is held digitally, in hard copy, or in another form.

Whenever you receive Personal Information from anyone you must:

- Treat the information as confidential.
- Ensure, to the extent possible, that the information is kept relevant, complete, up-to-date, and accurate.
- Protect the information from interference and unauthorised access and modification.
- Not disclose it to any third party unless the individual has consented to the disclosure and the disclosure is related to the primary purpose of Whiddon collecting the information.
- Not adopt a government related identifier (that is, an identifier that has been assigned by a government agency or state of territory authority; for example, a Medicare, Centrelink, or passport number) as its own identifier of an individual unless a legal exception applies, and this exception has been confirmed by your manager.
- File information away securely in the secure cabinets provided, or if the information is stored electronically, in accordance with our electronic filing systems.
- Not share information in public forums, including but not limited to, social gatherings or events, social media platforms (i.e., Twitter, Instagram, Facebook etc.) unless with express written, irrevocable, permission of the individual or a legal representative.

Who can I disclose personal information to?

In relation to clients, once a client has signed the Client Consent Form authorising disclosure you can disclose Personal Information to all the following persons:

- The client or the client's Authorised Representative
- The client's medical, nursing and care providers
- Whiddon's contractors and agents involved in providing Whiddon's products or services.
- Whiddon staff, where doing so is for the purpose of providing Whiddon's products and services.
- Persons nominated by the client on the Consent Form or otherwise expressly authorised by the client.

Never assume that a next of kin or a relative is the client's authorised representative or has authority to receive Personal Information. It is important to verify who we can disclose Personal Information to against the client's file.

There may be other situations where disclosure may be authorised by law even where the client has not signed a Consent Form. Never make a disclosure required or authorised by law until you have verified this with your manager.

In relation to individuals other than clients, you must never disclosure Personal Information to any third party unless it is directly connected to the primary purpose of us collecting the personal information from the individual. Always check with your manager.

You must never disclose any information to any individual if you believe that it may pose a threat to their health and safety; for example, if reading a client's file might cause them undue grief and might potentially lead to them engaging in self-harm.

If you believe that access should be denied on these grounds, you must always verify this view with your manager before acting upon it.

Disclosure of Personal Information to overseas recipients

Unless authorised by the individual or their Authorised Representative, no Personal Information should be disclosed or transferred overseas for any purpose other than providing Whiddon's products and services or where required by law.

If information is required to be sent overseas Whiddon will take reasonable steps to ensure that the overseas entity observes the APPs, Whiddon will need to enter a contract or memorandum of understanding that requires the overseas recipients and any subcontractors to comply with the APPs in relation to the disclosed information.

Whiddon may evaluate the security measures of both the agency and the overseas recipient to minimise the risk of unauthorised disclosure. (Australian Government Solicitor: Fact Sheet 29: Understanding and complying with the new Australian Privacy Principle 8 – Cross-border disclosure of personal information)

If you become aware of a situation where Personal Information may be transferred overseas you must immediately notify your manager prior to this disclosure so that your manager can obtain consent from the individual the Personal Information relates to or his/her authorised representative to the disclosure.

Open Disclosure

Whiddon acknowledges that from time to time, despite our best efforts, events or errors may occur either directly or indirectly with one of our aged care consumers, that results in feelings being hurt, or worse, adverse outcomes. Should any such incident, error or event occur, this may be confusing and traumatising. Whiddon believe under such circumstances, the resident or client and their family deserve "open disclosure", that is an explanation of what went wrong, why it went wrong, how it went wrong, a sincere apology and an expression of regret from an appropriate staff member of Whiddon. Whiddon promotes a culture where team members give comfort, support, and reassurance that it will not happen again or likely not happen again. Privacy is respected during open disclosure.

Direct marketing

Whenever Whiddon directly markets to an individual, we must provide a simple means by which the individual can opt-out of receiving such material. All digital marketing must be in accordance with the *Spam Act 2003* (Cth).

We may, from time to time, use your personal information for the purposes of sending marketing materials. We only do so in accordance with applicable laws or with prior consent. Recipients may opt out of receiving any marketing information from Whiddon at any time by telephoning on 1300 738 388 between 8.00 am and 7.00 pm Monday to Friday, or by emailing: hello@whiddon.com.au

If notification is received from an individual requesting that we no longer provide them with marketing material, notify your manager immediately so that steps are taken to ensure that the individual no longer receives such marketing material.

Social Media

Employees of Whiddon participate in social media activities. Whiddon reserves the right to monitor social media activities to the extent permitted by law, but it will also strive to protect employees' privacy where possible. Details can be found in Whiddon's social media usage policy: **available on MyStaffroom.**

Monitoring

See Whiddon's Information Technology information regarding email and web traffic monitoring and acceptable use.

How do I deal with requests for access and correction of Personal Information, including resident or client records?

Access requests

We are required by Australian privacy laws to provide clients, including former living clients, with access to information that relates to them. There are some legal exceptions, for example:

- Giving access would pose a serious threat to the life, health, or safety of any individual.
- The request is frivolous or vexatious.

- Denying access is required by law.

If Whiddon receives a request to access Personal Information we will endeavour to respond within 15 business days unless extenuating circumstances exist. Once a request is received the following procedure must be followed:

1. A request for access to an individual's information must be in writing addressed to:

   Frank Whiddon Masonic Homes of NSW
   Attn: Support Services - Executive Administration Team
   Locked Bag 7014
   Minto NSW 2566

   execadmin@whiddon.com.au.

   Each request must set out the full name and date of birth of the individual they are seeking records about. Each request must also be accompanied by sufficient evidence about the person's authority to access the information, including a copy of the identification of the individual to whom the access request relates.

2. Once a written request is received, it must be verified against our records to confirm that we continue to hold information about the individual.

3. If the client is not a current or former client or if we no longer retain records in relation to an individual, a written response should be sent to this effect.

4. If records are requested for a deceased clients these will be complied with according to the requirements in the section 'Deceased Clients' below.

5. If it has been verified that we do hold records pertaining to an individual, there is a valid request for access, and there is not a legal reason for denying access, then information will be released.

There is no fee to make a request to access Personal Information. However, if documents are copied, we will charge per page. The rate per page will be advised at the time of request.

If an access or correction request is refused, we must provide the requestor with a written notice explaining.

- The reason for refusal (except where it is unreasonable to do so); and
- Their options to raise a complaint.

Deceased clients

Please note that if a request for access relates to a deceased client, we must only release records if:

- We receive a subpoena; or
- The request is from:

- The executer of the deceased client's estate under a will which has been granted probate.
- An administrator of an estate which has been granted letters of administration if the client died without a will; or
- A person who has received written authority from the executor or administrator to access a deceased client's records.

Requests for access to a deceased client's records should:

1. Be made in writing.
2. State the name and address of the person making the request.
3. Identify the records which are being requested and the form in which the information should be provided (e.g., USB, email).
4. Include a copy of the requestor's drivers' licence, passport, or another photo identification.
5. Provide details of the executor of the will or administrator of the estate of the deceased client and include copies of all materials required to verify the details of that executor or administrator (e.g., A copy of the grant of probate and the will or letters of administration); and
6. Where the requesting party is not the executor of the will or administrator of the estate, provide the written authority from the executor or administrator.

All requests to be directed to:

Frank Whiddon Masonic Homes of NSW
Attn: Support Services - Executive Administration Team
Locked Bag 7014
Minto NSW 2566

Correction Requests

It is important to Whiddon that the Personal Information that it retains is up-to-date, accurate, complete, and relevant to the purpose of the use or disclosure. Whiddon must take reasonable steps to correct Personal Information that is inaccurate, out of date, incomplete, irrelevant, or misleading. If we have provided any Personal Information to a third party, we are required to notify them that we have updated or amended this information.

If we receive a request to correct Personal Information the following procedure must be followed:

1. A request to correct a client's information must be in writing addressed to:

   Frank Whiddon Masonic Homes of NSW
   Attn: Support Services - Executive Administration Team
   Locked Bag 7014

Minto NSW 2566

Each request must set out the full name and date of birth of the individual whose records they wish to correct. Each request must also be accompanied by sufficient particulars of why the correction is being sought and evidence of the person's authority to correct the information, including a copy of the identification of the individual to whom the correction request relates.

2. Once a written request is received, it must be verified against our records to confirm that we retain records in relation to the individual and that the correction sought is valid.

3. If the individual is not a current or former client or if we no longer retain records in relation to an individual, a written response should be sent to this effect.

No records should be amended or corrected without the express authority of the manager.

Privacy breaches and data breach response

A data breach is any (potential) unintended loss of control over or loss of personal data within Whiddon's environment. Preventing a data breach is the responsibility of all Whiddon's staff and contracted workforce. In addition, everyone is encouraged to notify their manager in case of an irregularity in relation to personal data processing activities. A timely discovery, response, treatment, and notification (of both regulatory authorities and potentially the individuals impacted) policy is outlined in Whiddon's data breach response policy.

A privacy breach might occur in several situations, for example:

- When there is a contravention of this Manual or Whiddon's privacy procedures, including any instructions from management concerning privacy and data management.
- When Personal Information is not updated or appropriately corrected
- When Personal Information in our possession or custody is lost or stolen
- When Personal Information is misused or subject to unauthorised modification or interference
- The attempt, successful or otherwise, to gain or assist any third party to gain unauthorised access to Personal Information or Whiddon's information systems.
- The refusal to co-operate with management in relation to any audit or privacy investigation.
- Through hackers or a computer virus that affects our internal computer systems and potentially compromises the Personal Information that we hold.
- Personal information shared on social networks is protected by the Privacy Act. Breaches of the Act on social media will be treated as a privacy breach.

Whiddon takes privacy breaches seriously. If you become aware of a privacy breach or a suspected privacy breach, you must immediately notify your manager.

Generally,[6], the actions taken following a data breach should follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.

Step 4: **Review** the incident and consider what actions can be taken to prevent future breaches.

At any time, entities should take remedial action, where possible, to limit the impact of the breach on affected individuals. If remedial action is successful in preventing a likely risk of serious harm to individuals, the NDB scheme notification obligations may not apply.

In general, Whiddon will:

- Take each data breach or suspected data breach seriously and move immediately to contain, assess, and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed.
- Undertake steps 1 (Contain), 2 (Assess), and 3 (Notify) either simultaneously or in quick succession. In some cases, it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs.
- Determine how to respond on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, Whiddon may take additional steps that are specific to the nature of the breach.

The following diagram summarises the data breach response process. The parts of this process that are required by the NDB scheme are coloured red.

[6] Australian Government Office of the Australian Information Commissioner – Privacy/ Part 3: Responding to data breaches – four key steps.

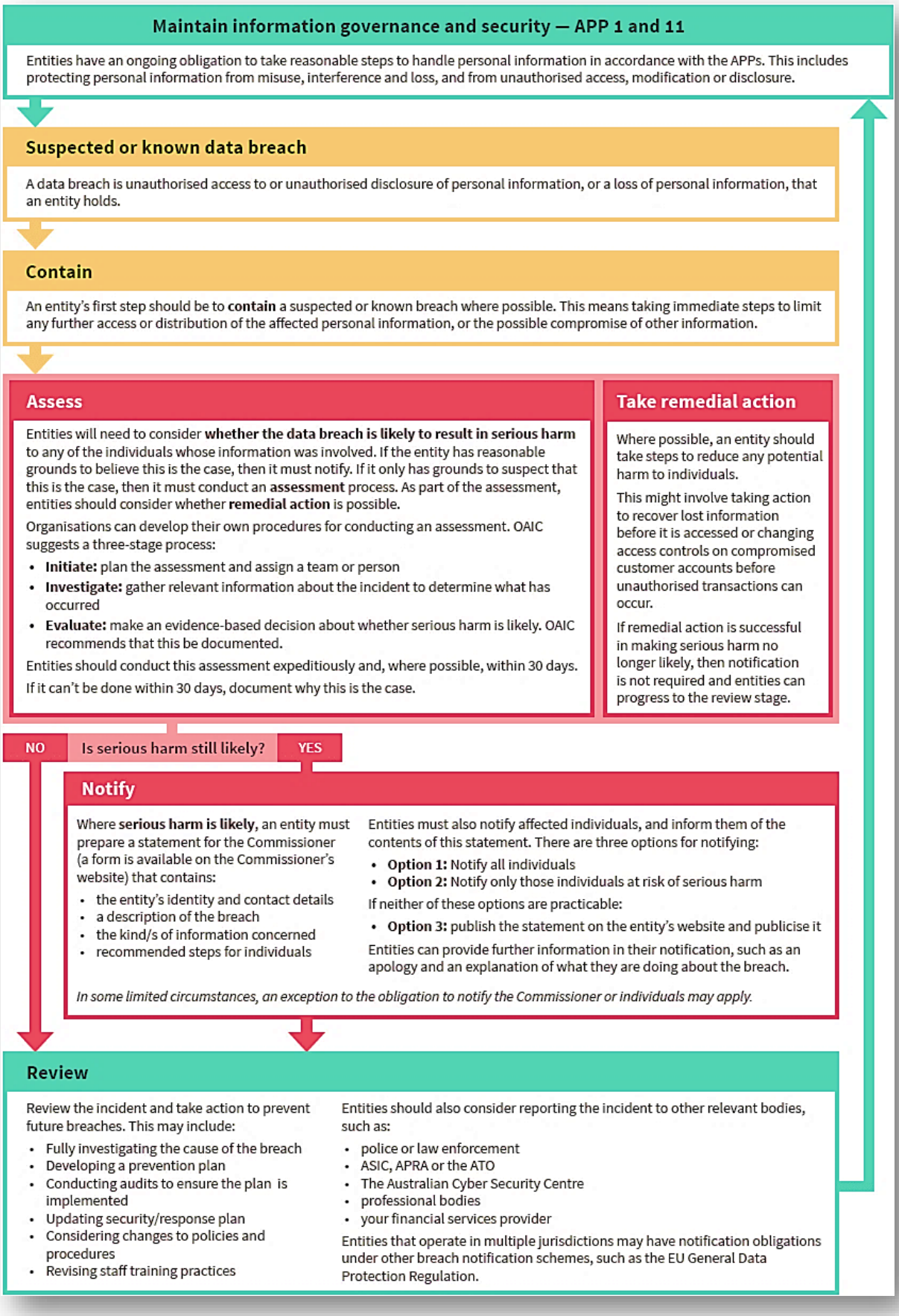

Figure 1 Data Breach Response Guide

Access to Privacy Policy

The Privacy Policy is freely available on Whiddon's website at www.Whiddon.com.au or an individual may request a copy by emailing execadmin@whiddon.com.au.

If an individual requests a hardcopy version of our Privacy Policy, you must provide them with a copy free of charge.

Complaints

If an individual would like to lodge a complaint about the way that Whiddon has handled or used Personal Information, in the first instance, the individual should be directed to make a written complaint to Chief Executive Officer Locked bag 7014, Minto NSW 2566. Email: execadmin@whiddon.com.au.

The complaint should include the following information:

- Summary of the privacy concern or alleged breach.
- Any action, or inaction, Whiddon has taken to try and resolve the issue; and
- Copies of any relevant documents associated with the complaint, including email communications that Whiddon may have provided.

Whiddon will endeavor to respond to complaints within fifteen business days unless extenuating circumstances exist.

Where relevant, responses to complaints should comply with Whiddon's 'Open Disclosure' process as outlined in this Manual.

Should an individual wish to take their complaint further they should be directed to contact the Office of the Information Privacy Commission. Complaints to the OAIC must be made in writing. The individual may be directed to the privacy complaint form and may submit it by:

Email: enquiries@oaic.gov.au
Post: GPO Box 5218, Sydney NSW 2001
Fax: 02 9284 9666

The individual may wish to discuss the matter first with the OAIC and can be directed to their telephone hotline as follows: 1300 363 992.

Privacy Audit

Each of Whiddon's complexes and facilities must conduct an annual privacy audit to certify that this Manual is being complied with. At a minimum the audit must ascertain:

- What sort of Personal Information is collected and held and whether this is appropriate.
- How Personal Information is collected.
- Where and how Personal Information is stored

- The appropriateness of security measures in relation to Personal Information stored or held by Whiddon.
- The persons or entities that have access to Personal Information

The Privacy audit is recorded in eQstats.