PRIVACY POLICY for Burke Property Agents

Instruction: This is a template to help you write a Privacy Policy for your agency. Instructions are shown in each section in green boxes like this and red type where you need to add your own agency name. Work though the document to ensure you have covered everything and that it reflects the practices in your agency.

OVERVIEW

The purpose of this policy is to ensure that Burke Property Agents manages personal and sensitive information responsibly, transparently, and in compliance with the Australian Privacy Principles (APPs) under the Privacy Act 1988. This policy outlines how personal information is collected, used, disclosed, stored, and protected by Burke Property Agents

This policy applies to all personal and sensitive information collected by in relation to clients, customers, personnel, contractors, and other stakeholders. It covers all methods of information handling, including Burke Property Agents digital, physical, and verbal communications.
Burke Property Agents is committed to protecting the privacy of individuals and ensuring the confidentiality, security, and integrity of personal and sensitive information. The agency will comply with the Australian Privacy Principles and other relevant legislation while fostering trust and transparency in all interactions.

Burke Property Agents complies with the Privacy Act 1988 (Cth) including the 13 Australian Privacy Principles (APPs) as outlined in the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth). Providing an overall framework for our privacy practices, *Burke Property Agents* has developed and implemented this APP Privacy Policy.

APPLICABLE LEGISLATION

This policy is designed to maintain requirements with additional jurisdictional requirements including:

- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth),
- Information Privacy Act 2014 (ACT),
- Privacy and Personal Information Protection Act 1998 (NSW),

AUSTRALIAN PRIVACY PRINCIPLES (APP)

Burke Property Agents manages personal information in an open and transparent way. This is evident in the implementation of practices, procedures and systems we outline in this policy, that ensure our compliance with the APPs and any binding registered APP code and provide suitable procedures for *(Name of your Agency)* personnel to be able to deal with related inquiries and complaints that may be received from time to time.

The following sections of this policy outline how we manage personal information.

Purpose Of Collection (APP1.4c)

INSTRUCTION: Clearly state the reasons for collecting personal information (e.g., to facilitate property transactions, manage rentals, provide property details, etc. An example is below: -

Burke Property Agents collects your Personal Information for the primary purpose of providing real estate services to our clients and marketing. We may also use your Personal Information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure. You may unsubscribe from our mailing/marketing lists at any time by contacting us in writing.

When we collect Personal Information, we will, where appropriate and where possible, explain to you why we are collecting the information and how we plan to use it.

You do not have to provide us with your personal information, however, if you do not, we may not be able to provide you with our services or information or allow you to any inspect property under our control.
We request the information from you so that we can provide you with the services and products you have requested from us, and the manage our obligations to you under any customer contract or applicable law. Some of the services we provide as a real estate agency include: -

- Any service or information we provide acting as an agent for the buying, selling, leasing, managing properties, or strata complexes:

- Marketing purposes and to provide you with information about products or services that may be of interest to you
- Enabling us to conduct our business, including meeting any legal or regulatory obligation placed upon us.

We will only collect your sensitive information if you have provided us with consent to do so. Where possible, we will give you the option of interacting with us anonymously.

The Kinds of Personal Information Collected and Held (APP1.4a)

Burke Property Agents collects personal information, which can include: -

- Contact information (name, address, phone number, email).
- Occupation
- Next of Kin (in case of emergency)
- Identification information (driver's license, passport details)
- Financial information (bank account details, income information)
- Rental and Employment references
- Property information (details of properties owned, rented, or being sought)
- Sensitive information such as credit worthiness and other details necessary to assess applications
- Other relevant information (marital status, family details, employment history).

How Personal Information is Collected and Held and Used (APP1.4b; APP1.4c; APP1.4f; APP1.4g)

We only use your personal information for the purpose for which it was provided to us, or

- related purposes that you would reasonably expect, and
- as permitted or required by law.

Such purposes would include: -

a) Internal Use

- In the ordinary course of conducting our business such as
  - Assisting you with purchasing, leasing or managing property
  - Responding to your enquiries and feedback
  - Informing you of property we have for sale or lease or may be open for inspection
  - Reporting to vendors or owners of properties that you, may have inspected or made enquiries about
  - Providing you with marketing information regarding the services we or third parties acting on our behalf provide.
  - Performing general administration or management functions
  - Any other purpose associated with our core function as a real estate agency

We may use the information to contact you by phone, email or text.

b) Disclosure to Third Parties

We may disclose your personal information to related companies, service providers, contractors' business partners other parties involved in the transaction, but only if one or more of the following apply:

- You have consented to the disclosure
- You would reasonably expect us to disclose your information this way
- We are authorised by legislation to do so
- Legislation requires us to disclose the information
- If an urgent health emergency or threat to life emergency arises

We do not ordinarily disclose or hold personal information overseas. If this becomes necessary, we will notify you and advise you of the country where the information will be sent or held, and the level of privacy protection in that country.

Burke Property Agents may use automated decision-making systems for the purposes of: -
Marketing for Sales and Property Management
Automated decision-making occurs when a computer program or AI is employed to make, or perform an action substantially related to making a decision. Such a decision may significantly affect your rights or interests. In the operation of these computer programs, personal information about you may be used to make decisions or take actions that are directly and substantially related to making those decisions and the services we provide.

As part of this automated decision-making process:

- The kinds of personal information used in the operation of such computer programs include your name and contact details
- The kinds of decisions made solely by the operation of such computer programs or AI may include Marketing for Sale listings and Property Management.
- The kinds of decisions for which a computer program or AI may assist (but not completely decide), that is substantial and directly related to making the decision, made by the computer program may include Prospecting for sale and Property Management Services.

Burke Property Agents ensures that automated decision-making is fair, transparent, and complies with the Australian Privacy Principles. You have the right to request information about any automated decisions that affect you and to seek human review of these decisions.

Website Analytics and Cookies

We may use website analytics tools to understand how people use our website, improve our services, and deliver relevant information or advertising. These tools are provided by third-party vendors, such as Google and others.

How information is collected

- Analytics tools may use cookies or other tracking technologies to collect information about your visits, such as pages viewed, time spent on the site, and device information.
- Information collected may include online identifiers like your IP address. When combined with other data, this may constitute personal information.

Vendors we use

- Google, Real Estate.com, Domain, TRA, Inspect Real Estate and RP Data

Purpose of collection

- To monitor and improve website performance
- To provide relevant advertising or marketing information
- To understand user behaviour and preferences

Opting out

- You can opt out of personalised Google advertising by visiting Google Ads Settings or through YourAdChoices.

Agency responsibility

- We keep this list of analytics providers and opt-out instructions up to date.
- If you do not want to be tracked by our analytics tools, you can disable cookies in your browser or follow the opt-out instructions above.

Data Security (APP1.4g; APP11)

Burke Property Agents has the following data security measures in place to protect your personal information from unauthorised access, use or disclosure.

All personal information collected by us through our platforms listed is stored in a variety of formats including electronically in databases, in hard copy files and on personal devices including laptop computers, mobile phones, cameras and other recording devices.

We take reasonable steps (both technical and organisational) to ensure that your personal information is stored both securely and is protected by: -

- Having a robust physical security of our premises and database/records/files.
- Taking measures to restrict access to only personnel who need that personal information to effectively provide services to you
- Having technical measures in place (e.g. anti-virus software, firewalls, the use of a VPN, secure payment portals, and the use of Secure Sockets Layer (SSL) protocols.

When your Personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify your Personal Information. Unless legislation requires otherwise, most of the Personal Information is or will be stored in client files which will be kept by us for a minimum of 7 years, in order that we can meet legislative requirements.

If you are sending us personal information, it is transmitted to us at your own risk. You must take the necessary steps to protect your information by protecting things like user names and passwords, customer details etc. You should notify us as soon as practical if you become aware of a security breach.

Data Breaches

If *Burke Property Agents* becomes aware of any security breach, an internal process will be immediately commenced in accordance with our Data Breach Response Plan. This will guide a conduct of an assessment of the breach and commence notification and rectification procedures if they are necessary.

Accuracy, Access and Correction of Personal Information (APP1.4d)

It is an important to us that your Personal Information is up to date. *Burke Property Agents* will take reasonable steps to ensure the information we collect and hold about you is accurate, up-to-date, and complete.
You may access the Personal Information we hold about you and update and/or correct it, subject to certain exceptions. If you wish to access your Personal Information, please contact us in writing.

If you believe or find that the information we have may not be up to date or is inaccurate, please advise us as soon as practicable so we can update our records and ensure we can continue to provide a quality service.

Burke Property Agents will not charge any fee for your access request but may charge an administrative fee for providing a copy of your Personal Information that we hold.

So that we may protect your Personal Information, we may require identification from you before releasing the requested information.

How do I Make Enquiries or Lodge Complaints? (APP1.4e)

If you have an inquiry or complaint relating to our Privacy Policy or compliance with applicable APPs please contact us using the contact details below. You will need to provide us with sufficient details regarding your complaint, as well as any supporting evidence and/or information.

We will refer your inquiry or complaint to our Privacy Officer whose details are below. They will, within a reasonable time, investigate the issue and determine the steps that *Burke Property Agents* will undertake to resolve any complaints. We will contact you if we require any additional information from you and will notify you in writing of the response or determination of our Privacy Officer.

If you are not satisfied with our response or determination, you can contact us or raise your concerns with the Australian Privacy Commissioner via www.oaic.gov.au.

If you believe we have breached the APPs or mishandled your personal information, or you have any questions about this Privacy Policy, please call immediately us on *02 95441111 or email michael@ burkeproperty.com.au*

Revision of Our Privacy Policy

We may revise this Privacy Policy or any part of it from time to time. Please review this policy periodically for changes. If We make significant changes to this policy, We may notify you using the contact details provided by you or by putting a notice on our website www.burkepropertyagents.com.au

Your continued use of our website, services, requesting our assistance or the provision of further personal or sensitive information to us after this Privacy Policy has been revised, constitutes your acceptance of the revised Privacy Policy.

How to Contact *Burke Property Agents*

Agency Name	*Cottenham Nominees Pty Ltd T/as Burke Property Agents*
ACN:	*88322285*
Licensee-in-charge	*Michael Christian*
Address:	*104 Cronulla St Cronulla*
Email:	*michael@burkeproperty.com.au*
PRIVACY OFFICER	*Michael Christian*
Email:	*michael@burkeproperty.com.au*
Phone No:	*02 95441111*
OAIC	1300 363 992 or www.oaic.gov.au

ATTACHED are several Notices that you can use as Privacy Notices where you collect personal information. There is one each for your website, Office and Open Homes.

FOR DISPLAY AT OPEN HOUSES OR PUBLIC INSPECTIONS

PRIVACY NOTICE

The Privacy Act 1998 regulates the collection and use, disclosure and maintenance of personal information collected by Burke property Agents from people attending Open for Inspections.

It is a condition of entry that before entering this property you must give your name and current telephone number to the Agency's representative. In addition, you also may give your email address.

This information we collect at this open house is collected for the following reasons: -

1. security reasons
2. to allow us to call, email or text you after the open for inspections to establish your interest in the property and to inform you of other properties we have listed for sale that may suit your needs
3. To send you information from time to time regarding the local property market
4. To enable us to give feedback to the vendor regarding interest in the property. In this case only your surname or given name will be disclosed
5. The information is used for internal purposes only and phone numbers and email addresses will NOT be disclosed to any other third party (except as in 3 above) without your written consent.

If you do not wish to be called as part of our normal follow up procedures, please advise the Sales Consultant before leaving.
All personal information we collect is held electronically and in hard copy in our office in a secure manner. It will only be used for the purposes noted above and will not be disclosed to any third party or recipients in other countries without your written permission, unless required by law. However, we are not liable for any unauthorised access of this information.

You have the right to

- view the information collected about you,
- the right to correct the information if it is not accurate, up to date or complete.
- Request secure removal of your information from our records

You may find our Privacy Policy on our website at: *www.burkepropertyagents.com.au*

If you want to obtain more information about our Privacy Policy, or view, correct or remove your information you may contact our Privacy Officer Michael Christian

p: 02 95441111
e: michael@burkeproperty.com.au

FOR DISPLAY IN YOUR OFFICE

PRIVACY NOTICE

The Privacy Act 1998 regulates the collection and use, disclosure and maintenance of personal information collected by ***Burke Property Agents*** from the clients, customers and the public.

Our Office collects various information from owners, vendors, potential tenants and landlords that includes: - name, contact details, banking details and other personal and sensitive information in order that we may service our clients and customers efficiently. We take reasonable steps to ensure the accuracy of the information we collect and that it is relevant and up to date.

This information we collect may be used for the following reasons: -

1. security reasons i.e. monitor and profile who is attending our office
2. to send news, information about our activities and general promotional material which we believe may be useful to you
3. to allow us to write, call, email or text you to inform you of properties we have listed for sale/lease that may suit your needs, and/or to keep you informed of developments in the real estate market
4. To enable us to give feedback to the vendor/owner regarding interest in a property that you have inspected. In this case only your surname or given name will be disclosed
5. To help us carry out the services we have contracted to provide by way of an agency agreement with you
6. The information is used for internal purposes only and will NOT be disclosed to any other third party without your consent, unless as noted in 3 above.

If you do not wish to be contacted as part of our normal follow up procedures or wish your information you provided us to be used to send you promotional material, you must immediately notify us.

All personal & sensitive information we collect is held electronically and/or in hard copy in our office in a secure manner. It will only be used for the purposes noted above and will not be disclosed to any third party or recipients in other countries without your written permission, unless required by law or noted in 3 above. However, we are not liable for any unauthorised access of this information.

You have the right to

- view the information collected about you,
- the right to correct the information if it is not accurate, up to date or complete.
- Request secure removal of your information from our records

You may find our Privacy Policy on our website at: ***www.burkepropertyagents.com.au***

If you want to obtain more information about our Privacy Policy, or view, correct or remove your information you may contact our Privacy Officer Michael Christian

p: 02 95441111
e: michael@burkeproperty.com.au

FOR DISPLAY ON YOUR WEBSITE WHERE INFORMATION IS COLLECTED

PRIVACY NOTICE

The Privacy Act 1998 regulates the collection and use, disclosure and maintenance of personal information collected by *Burke Property Agents* from the clients, customers and the public.

Our company collects various information from owners, vendors, potential tenants and landlords that includes: - name, contact details, banking details and other personal and sensitive information in order that we may service our clients and customers efficiently. We take reasonable steps to ensure the accuracy of the information we collect and that it is relevant and up to date.

This information we collect may be used for the following reasons: -

This information we collect may be used for the following reasons: -

1. security reasons i.e. monitor and profile who is attending our office
2. to send news, information about our activities and general promotional material which we believe may be useful to you
3. to allow us to write, call, email or text you to inform you of properties we have listed for sale/lease that may suit your needs, and/or to keep you informed of developments in the real estate market
4. To enable us to give feedback to the vendor/owner regarding interest in a property that you have inspected. In this case only your surname or given name will be disclosed
5. To help us carry out the services we have contracted to provide by way of an agency agreement with you
6. The information is used for internal purposes only and will NOT be disclosed to any other third party without your consent, unless as noted in 3 above.

If you do not wish to be contacted as part of our normal follow up procedures or wish your information you provided us to be used to send you promotional material, you must immediately notify us.

All personal & sensitive information we collect is held electronically and/or in hard copy in our office in a secure manner. It will only be used for the purposes noted above and will not be disclosed to any third party or recipients in other countries without your written permission, unless required by law or noted in 3 above. However, we are not liable for any unauthorised access of this information.

You have the right to

- view the information collected about you,
- the right to correct the information if it is not accurate, up to date or complete.
- Request secure removal of your information from our records

You may find our Privacy Policy on our website at: www.burkeproperty agents.com.au

If you want to obtain more information about our Privacy Policy, or view, correct or remove your information you may contact our Privacy Officer Michael Christian

p: 02 95441111
e: michael@burkeproperty.com.au

2. CYBER SECURITY

Other than Privacy, agents must be fully aware of the requirements about how they handle and keep data secure to ensure it does not get into the wrong hands or is accessed by unauthorised people.

The increased penalties came into force on 13 December 2022. The Privacy Act regulates the way personal information of individuals is handled by relevant organisations, otherwise known as Australian Privacy Principal Entities (APP entities). Refer to section 1 – Privacy for what organisations are covered by the fines.

NSW Fair Trading provides the following information to agents in regard to reducing the risk of data breaches in property agencies.

Improve your cyber security to reduce risks[1]

Property agencies collect and sometimes retain large amounts of personal information from customers. With major cyber incidents and data breaches affecting people across Australia, it's more important than ever that property agencies proactively work to improve cyber security to reduce risks. It's critically important that you understand your obligations which include storing personal information securely and making sure that it is destroyed or de-identified as soon as possible.

There are steps you can take to improve your cyber security and minimise the damage a potential cyber incident may cause to your customers and your reputation.

1. Urgently conduct an end-to-end review of your data security practices and systems. You may consider engaging an expert to identify cyber vulnerabilities and ways of reducing risks. This investment will pay off in the future.
2. Review your business processes to ensure you collect only required personal information.
3. Store personal information for the minimum time required and implement procedures for its safe disposal at the earliest appropriate time.
4. Assess the security of any third-party systems that your agency uses. Remember, their security practices will affect your business.
5. Evaluate the security of your data storage systems and upgrade them if necessary. All customer, client, tenant, and employee data should be stored with maximum security.
6. Mandate strong and complex passwords for all user accounts.
7. Ensure privacy obligations and cyber security is part of the annual training plan for all employees in your agency.
8. Familiarise yourself with Australian privacy law and ensure your business practices comply. This includes knowing your reporting obligations if personal information you hold is compromised.
9. Take the opportunity to inform your customers, clients, tenants, and employees that you're doing this important work because it's an urgent priority.

Engage your employees to help you

1. Work with your teams to secure their mobile devices (phones and tablets). These devices are essential tools of trade, but they can also be a risk.
    - Enable instant locking so the device isn't unlocked and accessible by others at any time.
    - Mandate passcodes at the maximum length for the device and operating system.
    - Engage multi-factor authentication for logins wherever it is available.
    - Ensure automatic operating systems updates are enabled on both personal and work-issued devices. This will install the latest security updates to protect from known vulnerabilities.
    - Give access to the minimum number of shared mailboxes on mobile devices.
    - Limit the number of people who have access to shared mailboxes and purge the information regularly.

[1] Source: https://www.fairtrading.nsw.gov.au/housing-and-property/property-professionals/running-a-property-agency/reducing-risks-of-data-breach-in-property-agencies as at 30 May 2024

2. Data breaches can occur when a folio, compendium, or hard copy document is lost or stolen.
   - Make sure that hard copy materials with physical signatures are stored in a locked location.

3. Develop a culture of reporting. Encourage your people to speak up if an incident may have occurred. Work with them to resolve the issue and make improvements.

Be prepared for the worst case

While it's important to be prepared for the time a cyber incident does occur, prevention is even better. When a cyber incident occurs, it requires an immediate, urgent, and unified response. In the same way that organisations run building evacuation drills, the best way to be prepared is to practise.

Identify people within your business who will be able to facilitate the urgent response and assign roles and tasks to team members. Be sure to integrate your drills into your business continuity planning. You may also be able to leverage resources available from your head office teams.

What to do if you experience a cyber-attack or data breach

If your agency experiences a cyber incident or data breach, help is available.

- Consider your obligations under the Notifiable Data Breaches scheme – Have a Data Breach Response Policy in place. See next section.
- Engage the team at the Australian Cyber Security Centre.
- Contact ReportCyber. Any malware or ransomware reports submitted are reviewed by the Australian Cyber Security Centre and if action is required police will be notified.
- If personal information may have been compromised, contact ID Support NSW.

3. DATA BREACH RESPONSE PLANS

In addition to abiding by the Privacy Principles another requirement of the Privacy Act is The Notifiable Data Breaches (NDB) scheme, which, requires organisations covered by the Act to notify affected individuals and the Australian Information Commissioner (OAIC) when a data breach is likely to cause serious harm. This scheme, introduced by the Privacy Amendment (Notifiable Data Breaches) Act 2017, came into effect on February 22, 2018.
A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

- a device with a customer's personal information is lost or stolen
- a database with personal information is hacked
- personal information is mistakenly given to the wrong person.

The notification to individuals must include recommendations about the steps they should take in response to the data breach. You should notify the OAIC using our online Notifiable Data Breach form.

For an Agency to protect itself in the event of a Data Breach it is strongly recommended that you have a Data Beach Response plan in place. A data breach response plan enables your agency to respond quickly to a data breach. By responding quickly, you can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.

A data breach response plan can help you:

- Meet your obligations under the Privacy Act
  Under the Privacy Act, an entity must take reasonable steps to protect the personal information that it holds[2].[1] A data breach response plan focussed on reducing the impact of a breach can be one of these reasonable steps.
- Limit the consequences of a data breach
  A quick response can reduce the likelihood of affected individuals suffering harm. It can also lessen financial or reputational damage to the entity that experienced the breach.
- Preserve and build public trust
  An effective data breach response can support consumer and public confidence in an entity's respect for individual privacy, and the entity's ability to manage personal information in accordance with community expectations.

[2] SOURCE: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-2-preparing-a-data-breach-response-plan#_ftn1

TEMPLATE for DATA BREACH RESPONSE PLAN

1. Introduction

Cottenham Nominees Pty Ltd t/as Burke Property Agents is committed to ensuring that your personal information of our clients and customers held by us is done so in accordance with the Privacy Act 1988, and the Australian Privacy Principles. Our Data Breach Response Plan provides the process we will follow by our staff if a data breach or suspected data breach happens within our agency.

The purpose of our Data Breach Response Plan is to establish a clear procedure for identifying, managing, and mitigating data breaches to protect all client information and comply with our legal obligations. It applies to all staff, contractors, and third-party service providers handling personal data within or on behalf of our office.

a. Definitions and Key Terms:

Agency	*Burke Property Agents ACN 88322285*
APPs	are the Australian Privacy Principles set out Schedule 1 to the Privacy Act, which apply to APP entities.
Assessment	is a key step in responding to a data breach, which should enable entities to make an evidence-based decision about whether serious harm is likely. Entities that are subject to the NDB scheme are required to conduct assessments of suspected eligible data breaches under s 26WH of the Privacy Act
Consumer Data Right	is regulated by Part IVD of the Competition and Consumer Act 2010 and associated rules, which aims to give consumers greater control over their data, by allowing them to share their data with accredited third parties.
Data breach	is the unauthorised access or disclosure of personal information, or loss of personal information.
Digital ID	is regulated by the Digital ID Act 2024 and associated rules and data standards, and aims to provide individuals with a voluntary, secure and easy way to reduce the sharing of their personal ID documents and instead verify their identity to access online government and private sector services.
Personal data	Personal information' is defined in s 6(1) of the Privacy Act, as information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable
Containment	
Notifiable Breach	is the unauthorised access or disclosure of personal information, or loss of personal information in circumstances where this is likely to occur, that is likely to result in serious harm to any of the individuals to whom the information relates (see s 26WE(2) of the Privacy Act).
OAIC	is the Office of the Australian Information Commissioner.
Remedial action	is the steps that an entity may take to prevent the likelihood of serious harm occurring for any individuals whose personal information is involved in an eligible data breach.
Sensitive information	is defined in s 6(1) of the Privacy Act to include personal information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. Sensitive information also includes all health information, genetic information, biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.

b. What is the Data Response Breach Plan

This data breach response plan (response plan) sets out procedures and lines of authority for our agency staff in the event the Agency experiences a data breach (or suspects that a data breach has occurred). A data breach occurs when personal information is accessed or disclosed without authorisation or lost.

Under the Notifiable Data Breaches (NDB) scheme the Agency must notify affected individuals and the OAIC (as regulator) when it has reasonable grounds to believe that there has been an eligible data breach of the entity.

An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an organisation or agency (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The organisation or agency has been unable to prevent the likely risk of serious harm with remedial action.

For good privacy practice purposes, this response plan is not restricted to eligible data breaches and covers any instances of unauthorised use, modification, interference with or loss of personal information held by (name of Agency). Data breaches can be caused or exacerbated by a variety of factors, impact different types of personal information and give rise to a range of actual or potential harms to individuals and entities.

This response plan is intended to enable the Agency to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals and to comply with the NDB scheme. Our actions in the first 24 hours after discovering a data breach are crucial to the success of our response.

The plan:

- sets out contact details for the appropriate staff in the event of a data breach
- clarifies the roles and responsibilities of staff
- documents processes to assist the OAIC to respond to a data breach.

c. What is a Data Breach

A data breach occurs when personal information is accessed or disclosed without authorisation or loss. A data breach may be on purpose or by accident. Examples include:

1. a misdirected email
2. a hack
3. disclosure over the phone
4. phishing attack.

2. Our Response Plan

Our Response Plan sets out the

a) Roles and responsibilities of staff
b) Contact details of staff
c) Procedures to be followed in the event of a breach

2a. Identify the Breach

If any staff member becomes aware of a suspected breach of private or sensitive information held by the agency the staff member must immediately: -

- Notify the Data Breach Manager of the suspected data breach
- Record and advise the Data Breach Manager of the suspected data breach
- Describe the type of personal or sensitive information involved
- If known the cause and the extent of the breach
- Any other known information regarding the breach

2b. Data Breach Response Team

POSITION	NAME	EMAIL	PHONE
Data Breach Manager	Michael Christian	michael@burkeproperty.com.au	02 95441111
Licensee in charge	Michael Christian	michael@burkeproperty.com.au	02 95441111
Legal Consultant	George Gourlas	ggourlas@gglawyer.com.au	02 95237507
Office Manager	Michael Christian	michael@burkeproperty.com.au	02 95441111
Privacy Officer	Michael Christian	michael@burkeproperty.com.au	02 95441111
IT Manager			
If Michael Christian is not available call David Kennedy 02 9544111 david@burkepropertyagents.com.au			

2c. Contain and Assess the Breach.

The Data Breach Manager must then assess and determine whether a data breach has occurred. The Data Breach Manager must

- If he/she has any suspicion that the breach looks to be a notifiable breach notify the licensee in charge
- with the approval of the licensee in charge must then engage the Agency's legal consultant to make an assessment and determine whether a data breach has occurred.

Where a minor breach is dealt with, the following details must be recorded in the Data Breach Incident Log:

a) Description of the breach or suspected breach.
b) Action taken by the Data Breach Manager and staff member to address the breach or suspected breach.
c) Outcome of that action.
d) Sign off from the licensee in charge that no further action is required; and
e) Confirmation that the incident has been recorded in the Agency's Data breach incident log.
f) If the breach is serious, it must immediately be escalated to the Response Team.

2d. Determination when Breach escalated to a Response Team

The following factors may determine when a data breach should be escalated to the Response Team:

- the number of people affected by the breach or suspected breach;
- whether there is a risk of serious harm to affected individuals now or in the future;
- whether the data breach or suspected data breach may indicate a systemic problem with the Agency's practices or procedures; or
- other issues relevant to the Agency's circumstances, such as the value of the data to the Agency or issues of reputational risk.

Once a matter has been escalated to the Response Team, the process outlined below must be followed.

NOTE: Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved and using that risk assessment as the basis for deciding what actions to take in the circumstances and in the future

2c. Response of Data Breach Response Team

The Data Breach Response team will undertake four steps in response to a data breach or suspected breach. The four steps are

- Contain
- Assess
- Notify
- Review and Re-evaluate

It is the Role of the Data Breach Manager to co-ordinate the following steps to be undertaken by the Response Team

STEP	DETAILS	RESPONSIBILITY
CONTAIN	1. Once a data breach has been identified, action must be immediately undertaken to contain it. Examples include: • Stopping an unauthorised practice by a staff member or third party • Recovering records • Shutting down the system to isolate the breach	Licensee in Charge
	2. Take immediate steps to limit or prevent any further compromisation of data	If IT breach – IT Manager

	3. Strategies to contain & assess a data breach: • How did the data breach occur? • Is the personal information still being shared, disclosed, or lost without authorisation? • Who has access to the personal information? • What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals.	Licensee in Charge/ IT Manager
	4. Designate person to coordinate response	Legal Consultant/ Privacy Officer
ASSESS	The Privacy Officer should move quickly to appoint someone to lead the investigation. It may be necessary to assemble a team that includes representatives from appropriate areas of the Agency in order to conduct the preliminary assessment. • INITIATE a plan and assign a team or person	Licensee in Charge
	• INVESTIGATE Gather relevant information about the following: - • What personal or sensitive information is involved • The cause and extent of the breach • What are the potential harms (to affected persons) of the breach	Privacy Officer/ IT Manager
	• CONTAINMENT. How can the breach be contained	Licensee in Charge/ Legal Consultant
	5. DATA COMPROMISED. What information was affected • Is it client information or Company information? • Who is affected by the breach? • Does the data that has been breached create a greater risk of harm? • What is the context of the affected information in the breach? • What parties have gained unauthorised access to the affected information? • Have there been any other breaches that could have a cumulative effect? • How could the information be used	Licensee in Charge/ Legal Consultant/ IT MANAGER
	6. CAUSE & EXTENT. Establish cause and extent of the breach • Is there a risk of ongoing breaches or further exposure of information? • Is there evidence of theft? • Was the information adequately encrypted, desensitised or otherwise not accessible? • Was the source of the breach accidental or intentional? • Has any or all of the information been recovered? • What steps have been taken to mitigate harm? • Is this a systematic problem or an isolated incident?	Licensee in Charge/ Legal Consultant/ IT Manager

	• How many persons or entities are affected by the breach? 7. EVALUATE • What is the harm to the affected persons and entities? • What are the harms to the Agency's business i.e reputational damage, legal liability, breach of Privacy Act 8. MITIGATE What steps can the Agency take to mitigate any risk of serious harm.	
NOTIFICATION	Undertake a Risk Analysis on in each case of a breach to determine whether the data breach notification is required. If it is likely notify: • Privacy Commissioner (OAIC) then • Affected individuals or entities Notification should be direct and occur in the usual way the Agency communicates with clients. If that is via email, the notice goes via email. If breach affects so many people that it is impractical to notify each separately, then the Agency must advertise [illegible] applies if the Agency does not have an individual's contact information or it is cost prohibitive to notify individually. The content of the notification will vary depending on the particular breach and notification method. However, the OAIC recommend that notifications should include the following information: • incident description • type of information involved • response to the breach • assistance offered to affected persons • other information sources designed to assist in protecting against identity theft or interferences with privacy (e.g. www.oaic.gov.au) • our contact details • whether breach notified to regulator or other external contact(s) • legal implications (e.g. the secrecy provisions) • how individuals can lodge a complaint with the Agency; and • how individuals can lodge a complaint with the OAIC (where the information is personal information). It may also be appropriate to notify other third parties, such as the police, cyber crimes, insurance providers, credit card companies, financial institutions, professional or other regulatory bodies, other internal or external parties who have not already been notified or agencies that have a direct relationship with the information lost/stolen.	Licensee in Charge/ Legal Consultant/ Privacy Officer

	NOTE: The 2024 changes to the Privacy Act now contain the concept of an apology. The Court, in determining whether there has been a 'serious invasion of privacy' will look at whether an apology was issued when it considers the amount of damages to award to a person. An apology in this instance is not deemed to be an admission of guilt or liability – but this comes with a warning – it is only in relation to 'serious invasions of privacy'. Speak with your Legal Consultant before actioning.	
REVIEW & RE-EVALUATE	1. Fully investigate the breach 2. REVIEW the incident and take steps to prevent future breaches and consider a prevention plan 3. Audit to endure prevention plan is implemented 4. Review third party providers who were involved in the breach 5. Update security/response plans that were involved in the breach 6. UPDATE Polies and Procedures and implement further training of staff if need identified.	Licensee in Charge/ Legal Consultant/ Privacy Officer

Appendix (if required develop these resources

- Templates: Breach notification forms, incident log templates.
- Forms: Internal reporting forms for staff.
- Resources:
  - Information on Notifiable Data Breaches: https://www.oaic.gov.au/privacy/notifiable-data-breaches.
  - Information of Data Breach Response Plans: https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/plans-policies-and-procedures/data-breach-response-plan