JERVIS BAY | MARITIME MUSEUM

PRIVACY POLICY

Purpose

1. This privacy policy describes the kinds of personal information the Museum collects and holds, how it is used and how it is secured.
2. It also outlines how a person may access information about themselves or seek correction of that information and how an individual may complain about a breach of an Australian Privacy Principle (APP).

Definitions

Personal Information

3. Personal information is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable:

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

Sensitive Information

4. Sensitive information is a subset of personal information. The Museum has a higher degree of responsibility when it comes to the collection and use of sensitive information. Sensitive information includes information about an individual's

    - health (including predictive genetic information)
    - racial or ethnic origin
    - political opinions
    - membership of a political association, professional or trade association or trade union religious beliefs or affiliations
    - philosophical beliefs
    - sexual orientation or practices
    - criminal record
    - biometric information that is to be used for certain purposes
    - biometric templates

Who should read this policy?

5. People who should read this policy include:

    - JBMM employees, members and volunteers;
    - contractors, consultants, suppliers or vendors of goods or services to the Museum;
    - applicants to the Museum for information under the Freedom of Information Act 1982; and
    - Individuals whose personal information may be collected, held, used or disclosed by the Museum.

Monitoring

6. This policy will be monitored by the Board and reviewed on a bi-annual basis.

Principles

Information collection purposes

7. The Museum collects information for a range of purposes that support our functions. This would include

    - Transactions that require customers to provide personal information, such as online transactions for the Museum Shop, Membership or pass holders, hiring a venue for personal events or donations to the Museum;
    - photographs, opinions and comments posted on the Museum's official social media platforms'
    - records of payments made, bank or credit card details for the purpose of payment and history of donations made;
    - personal information including photo ID, employment history, curriculum vitae and education information if applying for a position with the Museum;
    - certain health information; for example, food allergies or other medical needs such as access to facilities or events hosted by the Museum;
    - event registration information (including dietary requirements);
    - CCTV footage in areas where CCTV signage is located;
    - personal views and opinions about products and services through feedback.

8. The Museum will disclose at the time of collection how personal information will be used and handled.
9. JBMM is bound by laws which impose specific obligations when it comes to handling information. The organisation has adopted the following principles contained as minimum standards in relation to handling personal information.
10. JBMM will

    - Collect only information which the organisation requires for its primary function;
    - Ensure that stakeholders are informed as to why we collect the information and how we administer the information gathered;
    - Use and disclose personal information only for our primary functions or a directly related purpose, or for another purpose with the person's consent;
    - Store personal information securely, protecting it from unauthorised access; and
    - Provide stakeholders with access to their own information, and the right to seek its correction.

PROCEDURES

Museum visitor and client information

Association Members, Friends and Pass holders

11. Personal information is collected directly from the people who are interested in becoming Members, Friends or Annual Pass holders either via an application in hard copy or via phone or our website.
12. Personal information in our databases is used to:

    - distribute information about Museum events and activities;
    - maintain membership lists;
    - notify members regarding general meetings
    - notify members, friends and pass holders of renewals
    - Generate invitation lists for Museum events.

13. Members, Friends and volunteer data is stored in a secured internal database with hard copies stored in secure filing cabinets.
14. Emails sent to members, friends and volunteers regarding members business, general meetings and renewals use a secured internal storage for data and emails sent via Outlook. All emails sent are addressed to the Secretary and members and volunteers are forwarded as Blind Carbon Copies (BCC).

Museum customer relationship management system

15. The Museum maintains databases with contact details of individuals who regularly engage with the Museum or who wish to receive information about particular Museum activities.
16. Donors or people with a business-related interest in the Museum (for example, school teachers, people working in other cultural institutions, in the media or in tourism) are stored in external, secure online databases at Mail Chimp, an American based company that stores information on servers in the United States. (See mailchimp privacy policy/) and on the CRM HubSpot (See HubSpot Privacy policy).
17. Personal information is usually collected directly from the people who are interested in receiving the information or from a representative of their organisation.
18. Personal information in our relationship database is used to:

    - distribute information about Museum events and activities;
    - retain details of object and cash donors, and (with their consent) to publicly acknowledge those donors;
    - maintain a record of respondents providing feedback about their Museum experience;
    - generate invitation lists for Museum events.

19. Personal information on donors of Collection acquisitions is kept securely on file and in the CMC and is subject to Collections Management Policy.

Email marketing and promotional activities

20. All electronic communication from the Museum will be in accordance with the Spam Act (2003)
21. Individuals can choose to opt-out of receiving communications from the Museum at any point and Commercial electronic messages must contain a functional unsubscribe facility.
22. Unsolicited commercial electronic messages will not be sent.
23. Any Commercial electronic messages must include information about the individual or organisation who authorised the sending of the message.
24. Promotional material is sent to people on our data-base lists and can be used for a wide array of promotional activities.
25. Members, friends, stakeholders and general public sign up to receive this information via Annual Pass, Membership or direct email to JBMM.
26. Email marketing and e-news is delivered on either marketing platform MailChimp or CRM HubSpot. Further information is available at MailChimp's privacy policy or HubSpot Privacy policy)..
27. Address-harvesting software will not be supplied, acquired or used.

Bookings information

28. Bookings for functions, conferences, school visits and guided tours are regularly taken by the Museum. Only a limited amount of personal information is required to manage these bookings – such as first and last name, address and email address. The purpose of collecting this information is to ensure that an event or visit is properly coordinated. This information is not used for any other purpose (such as unsolicited marketing) without the consent of the individual concerned; however, the information may be used to generate broad demographic data.
29. The Museum uses South Coast Tickets or Humanitix most commonly as online booking system for events. The personal information provided by a customer to South Coast Tickets or Humanitix (excluding any billing or credit card information) is disclosed by South Coast Tickets or Humanitix to the Museum. The purpose of collecting this information is to ensure that an event or tickets are properly coordinated and accounted for.
30. South Coast Tickets is now powered by Humanitix software and Humanitix and its servers are located in Australia. People Using Humanitix are protected by Australia's Privacy Laws and Humanitix's privacy policy. Further information is available in Humanitix's privacy policy.

Visitor information and feedback

31. In order to improve its services, the Museum collects information from visitors about its programs. This information may be solicited (for example, through visitor surveys) or unsolicited (such as letters or emails from members of the public). The majority of evaluation that is initiated by the Museum allows people to respond on an anonymous basis. Visitor surveys, which the Museum regularly uses to seek feedback from visitors, do not involve the collection of information that could lead to a person being identified, although more generic information such as age and city of residence may be collected for demographical analysis. Respondents have the option of providing their personal

information to the Museum if they wish to join the Membership program or subscribe to a mailing list.

32. Where members of the public provide their personal information to the Museum in the course of making an enquiry or comment, that information will only be used by the Museum to deal with the person's enquiry or comment. Personal information in the form of photographs of visitors is collected only with the consent of the person or their parent/guardian. The consent forms for photography include the name of the person in the photograph and their contact details.

Historical collection, exhibition and research information

33. The Museum collects personal information relating to objects in its collections and on loan to the Museum. This information includes details about an object's history, including its current and previous owners and other people connected with the object. The purpose of collecting this information is to assess an object's ownership and provenance prior to acquisition or loan.
34. Personal information about an object is obtained from a range of sources including from the donor/vendor and from historical records. The nature of this research is such that personal information is not always collected directly from the person to whom the information relates but from other sources such as third party oral or written histories or newspaper or magazine articles. Personal information may also be collected in the course of historical research conducted by the Museum and for the purposes of exhibition. Such information may not necessarily relate to an object in the Museum's collection. This information is maintained in a range of forms, for example in writing, as video or sound recordings, or photographs.
35. The Museum may collect limited personal information for the following purposes:

    - to facilitate the management (eg transportation and insurance) of an object;
    - to arrange physical access to the collection by researchers, family members, Indigenous community members or special interest groups;
    - to respond to enquiries for historical information received from members of the public
    - to meet obligations under legislation, such as the Firearms Act or the Poisons and Therapeutic Goods Act.

36. There is an exception in the Privacy Act for materials kept in a library, art gallery, or museum for the purposes of reference, study or exhibition. Examples include photographs of individuals used in an exhibition or letters containing personal information kept in the Museum's collection. The Museum will, where possible, provide advice regarding this exception during the accessioning process.

The Museum's website

37. The Museum has an Association website and Museum-identified spaces social networking site Facebook.
38. The Museum's website may use cookies for the purpose of collecting statistical data. This will help the Museum determine if you have visited the website in the past. The Museum will also collect data such as IP addresses, date and time of visitation and which parts of the website you have explored. The Museum will not attempt to identify anyone

browsing the website unless they are logged into an account they have created with the Museum.

39. The Museum website currently uses Muse Software but will upgrade to Wordpress or Drupal.
40. The Museum's website refers to this privacy policy and conditions of use statement. Personal details are maintained on secure servers.

Personnel and administrative records

41. The Museum collects personal information about its employees, volunteers, interns, contractors, and Board members. The purpose of collecting this information is to properly administer matters relating to a person's employment or duties at the Museum.
42. Prospective employees and volunteers provide the Museum with personal details employment history, curriculum vitae and professional references.
43. Employee records usually include personal details (such as full name, addresses, email address, contact number and next of kin details), bank account details, tax file number, employment history, medical checks, police checks, leave, salary and superannuation records. Records may also be kept in relation to rehabilitation or worker's compensation claims, discipline or code of conduct matters, and performance management. This information is kept and stored in the Museum's personnel information management system and is only accessible to authorised staff
44. Volunteers provide the Museum with their personal details (such as full name, addresses, email address, contact number and next of kin details). Centrelink applicants that come from a provider either have a working with children check or police check. Volunteers may also provide an employment history, curriculum vitae and a copy of their driver's licence. This information is used to assess the suitability of people to become Museum volunteers which may include medical checks and police checks. This information is kept and stored in the Museum's personnel information management system and is only accessible to authorised staff.

Security records (including CCTV)

45. The Museum uses closed circuit television (CCTV) systems to monitor and record activity in a range of publicly accessible locations at the Museum. The purpose of this monitoring is to provide a safe and secure environment for Museum staff and visitors and to protect the Museum's collections and exhibits from damage, theft or loss.
46. The images recorded by the cameras may include identifiable images of people visiting the Museum. These images are stored in a secure environment, and access to these recordings is limited to authorised staff only. CCTV footage is held on a 3-month rolling basis.
47. Where an incident has occurred warranting further investigation, the Museum will allow the recording to be viewed by people responsible for investigating the incident, both within the Museum and/or external investigative bodies or law enforcement agencies (such as Police NSW).
48. Signs have been placed at all public entrances to the Museum advising that the cameras are in operation.

Museum Shop

49. The Museum uses a third party provider, Lightspeed, to collect personal information when purchases are made via the Museum's online shop. Customers may also leave their details in order to purchase items by mail order while at the retail store. This is stored directly into Lightspeed's database. Personal information is collected for the purposes of fulfilling the order and, if the purchaser has asked to receive newsletters or other information about the Museum, to provide them with that information. Further information is available in Lightspeed Privacy Policy
50. Personal information may be disclosed to Australia Post or another couriering company for the purposes of delivering an order. The Museum also retains order details (excluding credit card details) in our third party application, Lightspeed to help manage any returns, refunds or exchanges. Where a refund is required, The Museum will contact their bank merchant to authorise this refund back to the customer account.
51. Customers may also leave their details in order to have items placed on hold. This information is destroyed immediately once claimed at the retail shop.

Collection and storage of sensitive information

52. Sensitive information may be collected in relation to some employees or Volunteers. For example, employees may formally identify as a person of ethnic descent, or as having a disability. Health information (for example medical reports or certificates) may also be collected by the Museum where there is a workers' compensation or other health-related matter affecting an employee, as well as to conduct pre-employment medical checks.
53. National police history checks maybe conducted on prospective staff members, volunteers, interns, visiting researchers and contractors or for the issuing of a Museum keys. The individual's written consent must be obtained before a check is submitted and processed, and access to relevant personal information is strictly limited to authorised Museum staff.
54. Incident reports are required to be completed when a security incident, an injury or hazard has occurred or been identified. These reports may contain information, some of a medical nature, about visitors, volunteers and staff.
55. The Museum may hold information about a staff member's union membership if that person has authorised a deduction from pay for their union dues. There may be other records, which would identify union members such as right of entry permits, email communication between union members, or where union delegates are represented on Museum committees
56. These records are stored in a secure environment, and access to these records is limited to authorised staff only.

.

Third Party Information Collection

57. When the Museum uses third parties to collect personal information, they will be bound by their own privacy policies and the laws in the countries in which they are hosted.
58. The information transferred and stored in the Museum's databases will be handled in a secure environment.

Dealing with us anonymously or pseudonymously

59. There are circumstances where there is an option to remain anonymous or use a pseudonym when interacting with the Museum. For example, providing feedback. If circumstances are such that you cannot deal with the Museum anonymously or pseudonymously, an explanation will be provided, and there will be an option to opt-out of further contact.

Usage and disclosure of personal information

60. Personal information will be used for the particular purpose for which it was collected.
61. The Museum will not use or disclose your personal information for any other purpose unless you provide your consent or it is required, or authorised, by law

Integrity of personal information

62. Electronic personal information will be stored on secure systems, accessible only by employees and contractors with a genuine business need to access it. When personal information is kept in hard copy, it will be kept securely in locked cabinets or in secure storage when not in use.
63. If personal information needs to be disposed of, the Museum will use secure methods of destruction and disposal

Overseas disclosure of personal information

64. Where necessary, the Museum may disclose or store personal information with overseas third parties, including suppliers and database hosting services. Individuals will be notified at the time of collection and may choose to opt-out of providing the Museum with their details.
65. If the Museum is required to disclose personal information to an overseas third party under international law, it will ensure that this is done in accordance with the Australian Privacy Principles, and, where possible, individuals will be informed of the disclosure.

Notification of breach

66. The Museum will endeavour to notify users about any kind of data breach as soon as practicable. The Museum has developed procedures to be applied in the event of a data breach, based on the procedures implemented by the Australian National Maritime Museum. The procedures are provided in the Attachment.

Complaints and Access

Complaints

67. The Museum will take reasonable steps to deal with enquiries or complaints about compliance with the Privacy Act. The Museum will acknowledge receipt of a complaint within 14 days and send a considered response to complaints or suggestions within 30 days. The Museum is committed to quick and fair resolution of complaints and will ensure

that all complaints are taken seriously. The Museum may take a longer period to address a complaint where an individual has agreed to it in writing.

68. Complaints about the Museum's personal information handling practices may also be made to the Office of the Australian Information Commissioner.

Access and Correction

69. Under the APP, individuals have the right to access and correct their personal information stored by the Museum. The Museum will respond to access requests within 30 days. There are no charges imposed on requests for access to personal information and correction of personal information. The Museum strives to ensure that personal information is accurate, up-to-date, complete, relevant and not misleading.
70. If the Museum cannot provide access to personal information, for example, if the information has been legally and securely destroyed in accordance with procedure, a written explanation will be provided.

Responsibilities

Privacy Contact

71. The Museum's Board is responsible for maintaining this policy. The Board is also responsible for providing advice on privacy issues; acting as the point of contact for the federal Privacy Commissioner; and investigating any privacy complaints. For further information, please contact Secretary@jbmm.asn.au

Agreed by the Board of LDHCH Inc on 8 May 2023

Jervis Bay Maritime Museum

Data Breach Procedure – 2023

1. Scope

1. Scope

1.1 Background

The Notifiable Data Breaches (NDB) scheme came into effect on 22 February 2018. It applies to all agencies and organisations covered by the *Privacy Act*, which includes the Jervis Bay Maritime Museum ('the Museum').

The NDB scheme establishes a notification scheme for data breaches that are likely to result in serious harm. Under the scheme, individuals whose personal information is involved in such data breaches must be notified of the breach and the steps taken in response to the breach. The Australian Information Commissioner ('the Commissioner') must also be notified of the data breach.

1.2 Definitions

1.2.1 Data Breach

Unauthorised access to, or unauthorised disclosure of, personal information or a loss of personal information. A data breach can be accidental or deliberate.

1.2.2 Notifiable data breach

A notifiable data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by the Museum (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 Museum has been unable to prevent the likely risk of serious harm with remedial action.

1.2.3 Unauthorised access

Unauthorised access occurs when the following criteria is met:

- Personal information is accessed by someone who is not permitted to do so. This includes access by any of the following:
  - Employee
  - Volunteer
  - Independent contractor
  - An external third party such as a hacker.

Examples:

- An employee browses sensitive customer records without legitimate reason.
- Personal information is accessed in an external IT attack.

1.2.4 Unauthorised disclosure

Unauthorised disclosure occurs when the following criteria is met:

- Personal information is made available to others outside the Museum. This can be either intentional or unintentional

Example:

- An employee or volunteer accidentally sends a letter with Member A's membership information to Member B.

1.2.5 Loss of personal information

- Loss of personal information occurs when the following criteria are met:
- Hardcopy or a device containing soft copies of personal information is lost.
- In a location or in a way where that information can be accessed or disclosed to unauthorised persons.

Examples:

- An unencrypted USB stick containing a spreadsheet of personal information is left on public transport.
- Completed membership forms are thrown away in the regular rubbish bin and taken to a public waste disposal centre.

1.3 Monitoring

This procedure will be monitored by the Museum Director, and formally reviewed every two years, unless otherwise required.

2. Assessment Process

2.1 Decision Makers

The Australian Information Commissioner has enforcement powers under *Privacy Act* including receiving complaints from individuals, conducting investigations and issuing directions to an agency. Given the consequences of non-compliance with the NDB scheme, only the Museum staff/volunteers listed below are responsible for determining whether a data breach is likely to result in serious harm and should be notified under the scheme. This includes:

- Director
- President
- Secretary
- Board members

2.2 Likely to result in serious harm

In order to determine if there is a likelihood of serious harm, the decision maker should assess the nature of the breach, the type of information collected and the scope of the breach. Some examples of serious harm include:

- financial fraud, including unauthorised credit card transactions or credit fraud
- identity theft
- physical harm or intimidation, including family violence
- reputational, psychological or emotional harm

The decision maker should then assess the following three factors to determine whether there is a notifiable data breach:

2.2.1 The type of personal information involved in the data breach

Some personal information is more sensitive than other information and could lead to serious ramifications for individuals if accessed. Information about a person's health, criminal history, documents commonly used for identity fraud (for example Medicare card, driver's licence) or financial information are examples of information that could easily be misused if the information falls into the wrong hands.

2.2.2 Circumstances of the data breach

The scale and size of the breach may be relevant in determining the likelihood of serious harm. The disclosure of information relating to a large number of individuals would normally lead to a higher risk of at least some of those people experiencing harm. The length of time that the information has been accessible is also relevant.

Additionally, an assessment of who may have gained unauthorised access to the information and their intentions should occur. For example, a hacker might access data maliciously and intend to cause harm, while a contractor may have accessed this data to email the individual about a work related matter.

2.2.3 Nature of possible harm

Consider the broad range of potential harm that could follow from a data breach including:

- identity theft
- financial loss
- threat to a person's safety
- loss of business or employment opportunities
- damage to reputation (personal and professional).

The more comprehensive the data set compromised, the more possible categories of harm and the higher the likelihood of serious harm. For example, a list of customer names, email addresses, phone numbers and post codes is more likely to generate serious harm than one of those categories of information alone. De-identified and highly generalised information in isolation, such as post codes, may not rise to the level of a notifiable breach.

2.3 What to do if a data breach is suspected but not confirmed

The notification requirements apply where there are reasonable grounds for believing that a data breach has occurred.

If it is unclear whether a data breach has occurred, but there is a suspicion that there may have been a breach, staff need to act quickly. Once it is suspected that there may have been a breach, the *Privacy Act* requires that an assessment of the situation be made as

soon as practicable (within 30 days) to determine if there has been a data breach requiring notification.

The assessment process should involve:

- deciding whether an assessment is necessary and who should carry it out
- quickly gathering relevant information about the suspected breach
- deciding whether an eligible data breach has occurred and if so, following these procedures.

Remember that steps can be taken to mitigate potential harm at any time. If remedial action is successful in preventing serious harm, notification is not required.

2.4 Who should the data breach be reported to?

Staff who initially become aware that a data breach has occurred, or suspect that one has occurred, must immediately inform the Museum Director. They should make a record of:

- the time and date the breach was discovered or suspected;
- the type of personal information involved;
- the cause and extent of the breach;
- any other relevant information.

If a data breach is suspected or known to have happened, the staff member and/or the Museum Director must advise the President and Secretary as soon as practicable.

2.5 Remedial action

Action should be taken as soon as possible to contain a suspected or known breach. This involves taking immediate steps to limit any further access to or distribution of the information. Such action might involve recovering or locating lost information before it is accessed or changing controls on IT accounts. For example, a lost phone might be remotely wiped of data.

There is no need to notify individuals or the Australian Information Commissioner of data breaches if the Museum has taken remedial action, and as a result the data breach would not be likely to result in serious harm. Whether the remedial action is sufficient should be considered in the earliest stages of the data breach by the Museum Director, in consultation with the President and Secretary.

2.6 Establishing a data breach response team

A data breach response team should be established as soon as possible once it is determined that a data breach is likely to require notification of affected individuals.

The role of the response team is to:

- take action to contain the breach
- ensure evidence/information is collected and preserved
- conduct an investigation to determine when and how the breach occurred, the type of information involved, the cause and extent of the breach, the individuals affected and the risk of serious harm
- decide who needs to be made aware of the breach
- decide whether to notify affected individuals, how the notification should occur and the contents of the notification

- report to the Board on the outcome of the investigation and any recommendations.

The Museum Director will coordinate the team's response and advise the Board as required. If the Museum Director is unavailable, the next nominated individual relevant to the breach will handle the matter.

The composition of the response team will depend on the size, nature and complexity of the breach. Representatives of the operations area responsible for the personal information involved in the data breach would usually be a part of the response team. For example, a data breach relating to the membership program would mean that the Secretary would be on the response team.

If data breach involves personal information relating to customers or employees of an agency receiving services from the Museum, for example, another museum or cultural institution, a representative of that agency should be involved. Where required, expert external advice (for example specialised IT security services) may also be sought if not available within the Museum.

2.7 Record keeping

Records of the data breach and the response team's actions should be kept in the authorised records management system.

3. Notification Process

3.1 Notification

If the Museum has responded quickly to the breach, and as a result of this action the data breach is not likely to result in serious harm, there is no need to notify individuals or the Australian Information Commissioner. However, the Museum may decide to tell individuals about the incident if it is considered appropriate.

Where serious harm is likely, the Museum Director/President will advise affected individuals and the Australian Information Commissioner of the type of breach, the information it relates to and recommended steps for individuals to minimise the risk of serious harm.

3.2 Notification Methods

The Office of the Australian Information Commissioner (OAIC) has created a Notifiable Data Breach Form. Completing this will satisfy the obligation to notify the commissioner of a notifiable data breach.

There are three options for notifying individuals:

1. Notify all individuals whose personal information is affected
2. Notify only those individuals at risk of serious harm
3. If neither of the above are practicable, publish a statement on the Museum's website and further publicise it via other means, for example social media or media release.

Deciding which option to use to notify individuals will depend on the time, effort and cost involved. If it is not possible to assess which particular individuals are at risk of serious harm, all individuals who are impacted by the breach should be notified. Where the response team determines that only a subset of people are at risk of harm, it may be better to notify only those individuals to avoid causing unnecessary distress to individuals who are not at risk.

Individuals should be contacted using the method of communication normally used by the Museum to communicate with them. Individuals can be notified by email, SMS, telephone call or letter. If contact details for the person are available, direct communication is appropriate. If contact details are not available, then a message on the Museum's website or via social medial channels may be the best way of notifying affected individuals.

The notification must include as a minimum the following:

- the name and contact details of the Museum
- a description of the data breach including when it occurred, the circumstances of the breach, who may have accessed the information and the steps taken to contain the breach
- the kinds of information concerned
- recommendations about the practical steps (if any) that affected people should take in response to the breach.

3.3 Notification time frame

It is expected that the Commissioner and affected individuals will be notified as soon as practicable of a breach, taking into account the complexity, time and resources required to prepare a statement. The Museum will contact any affected individuals as soon as practicable.

Rectification of a data breach can be concurrent with the notification process.

4. Review and follow up

The response team should review the incident and make recommendations about how to prevent future breaches. This may include updating policies or procedures, revising or conducting additional staff training or changing IT access controls. Where additional risks are discovered through a data breach, relevant policies or procedures should be updated to reflect the new risk or threat and potential mitigations.

5. Definition of responsibilities

Australian Information Commissioner is responsible for receiving notifications of eligible data breaches, encouraging compliance with the NDB scheme, handling complaints, conducting investigations, and taking action in response to non-compliance.

Decision Maker is a person with responsibilities for assessing the severity of a data breach and the response the Museum should take to remediate and notify.

Museum Staff are responsible for identifying and reporting potential data breaches.

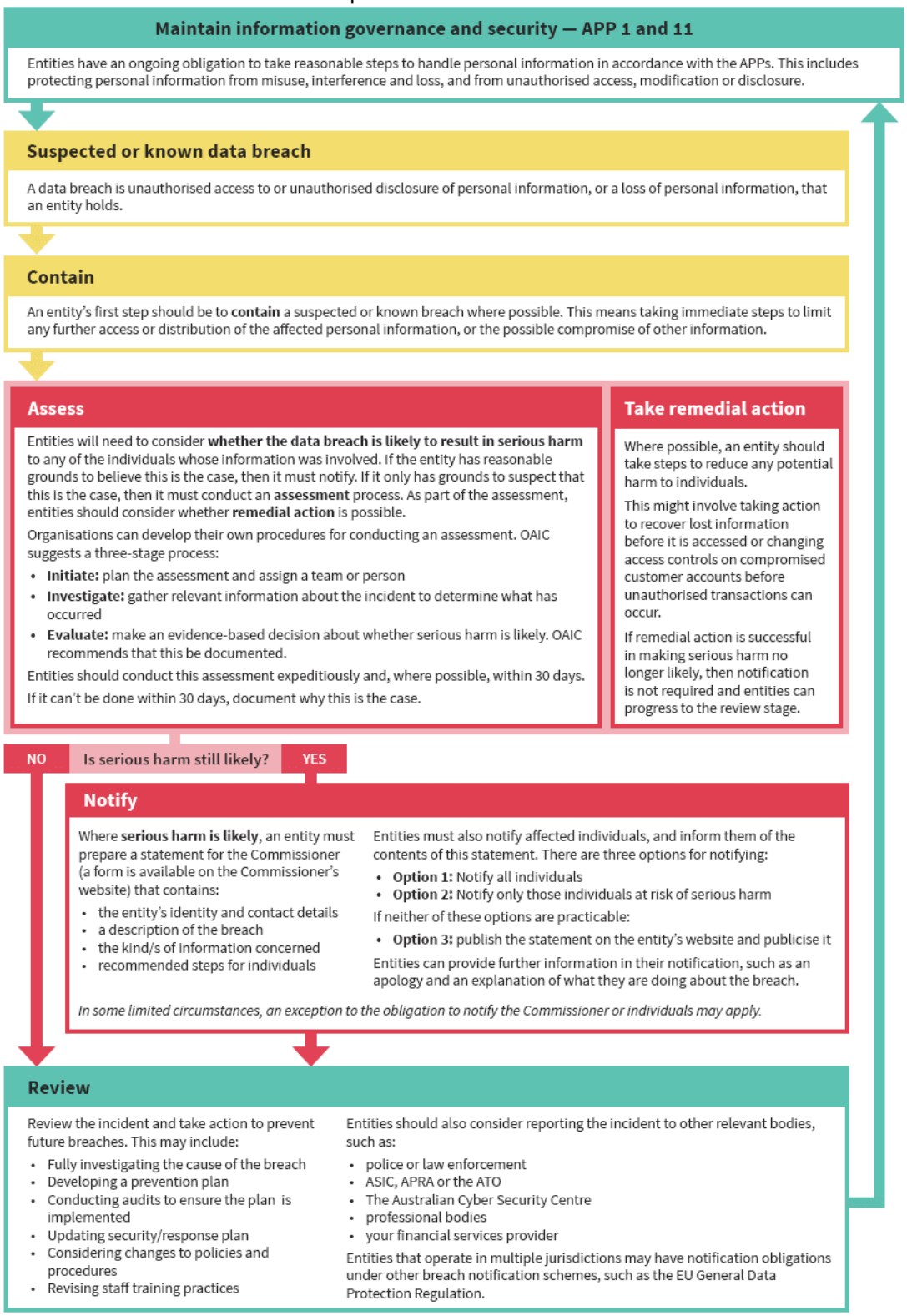
6. Relevant policies

This procedure supports the following policies:

- Privacy Policy

Appendix A

Flowchart: OIAC's Data Breach Steps



Appendix B

Template: Sample Data Breach Notification

Every data breach notification is required to include the following information:

- Our name and contact details
- A description of the breach, including:
  - the date, or date range, of the unauthorised access or disclosure
  - the date the Museum detected the data breach
  - the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure)
  - who has obtained or is likely to have obtained access to the information
  - relevant information about the steps the Museum has taken to contain or remediate the breach.
- The kind or kinds of information involved in the breach
- The steps we recommend individuals take in response

The format of this message can change. If a breach affects only a small number of people, a phone call or letter might be used. For breaches that affect larger numbers of people, text messages, emails, posting on the website, notifications on social media, etc may be options. This is up to the discretion of the business unit with advice from the Privacy Officer on duty.

Data breaches must be notified to the OAIC. The form for this purpose is provided here.

Sample Data Breach **Notification**

Jervis Bay Maritime Museum
2 Dent St,
Huskisson
NSW
2540

Dear *[insert name ie. Mr Joe Smith]*,

We wish to inform you that we have experienced a data breach and you have been identified as being affected by the breach.

From [Insert date range of breach, ie. 13th May 2018 – 7th July 2018] the *[Identify the type of breach including a brief description of what happened ie. Welcome Wall Database was accessible to all staff who had an employee email account. The error was due to a defect which occurred during a system upgrade to the Welcome Wall database.]*

This was identified on the *[insert date of discovery of breach including a description of what has been done to mitigate breach since ie. 7th of July and the access was immediately revoked and improved security protocols have been enforced, including a… <provide details>]*

The compromised information includes *[insert details of personal information which was exposed and what was not ie. names, addresses, phone numbers and dates of birth. Your payment details are kept encrypted on a bank processing server and are unaffected.]*

Investigations have been undertaken, and it is confirmed that there was unauthorised access to this information by *[insert suspected person ie. unknown persons.]*

Due to the risk of *[insert potential risks ie. identity theft and malicious activity*], we are encouraging all affected individuals to *[insert recommendations to mitigate harm ie. change passwords, run a credit check and … <provide details that have been advised by experts in the field>.]*

We apologise for this breach. We take your privacy very seriously and encourage you to contact us if you have any concerns or comments. Please contact *[insert operations area details here ie. Membership Secretary@jbmm.asn.au]*

For any escalations, please contact *Secretary@jbmm.asn.au*