PRIVACY POLICY

Issue No:	4.0
Dated Issued:	March 2014
Reviewed:	September 2018
Next Review Date:	September 2020
Document Status:	FINAL
Prepared by:	Rebecca Kenny, General Counsel
Approved by:	The Executive
Document Reference:	A/59518

CONTENTS 2

INTRODUCTION

The Australia Council for the Arts (ABN 38 392 626 187) (**us, we, our**) maintains a policy of strict confidence concerning your (**you, your**) personal information.

This Privacy Policy has been developed in accordance with the Commonwealth *Privacy Act 1988* (**Privacy Act**). We have also taken steps to ensure that, if you tell us you are located in the European Union (**EU**), we will seek to give you the protections available to you under the *General Data Protection Regulation* (**GDPR**). Together, we refer to these two pieces of legislation as "**Privacy Law**".

The Privacy Policy applies to the collection, storage, use and disclosure of your personal information by us. Access to our website http://www.australiacouncil.gov.au (referred to in this Privacy Policy as **our website**), or use of our services, is conditional on your acceptance of the terms of this Privacy Policy. This Privacy Policy applies to information provided to us whether via our website or any other means and demonstrates how we will comply with the Privacy Law, including the Australian Privacy Principles under the Privacy Act.

Although we will comply with this Privacy Policy in respect of information provided to us by persons under the age of 18 years, those persons must obtain the consent of a parent or guardian prior to using our website and the parent or guardian will be responsible for appropriately supervising the person's use of our website.

If you have any further questions or if you wish to receive more information on our information practices and use of our Privacy Policy, please contact our Privacy Officer at: privacyofficer@australiacouncil.gov.au.

COLLECTING PERSONAL INFORMATION

The Australia Council collects personal information in order to fulfil its obligations as set out under Section 9 of the *Australia Council Act 2013*.

The types of personal information we collect include contact details such as the name, email, phone and mailing address of individuals. We may also collect date of birth, identification details, professional, education and employment information, Australian Business Numbers (ABNs), bank details and payment transactions.

If it is reasonable and practical to do so, we will collect personal information directly from you. This will include contact details and other information relevant to providing services to you. This may occur in a number of ways, such as when you make a grant funding application, register to become a peer assessor, subscribe to our communications, provide contract services, make an employment application or otherwise contact us regarding the functions of the Australia Council for the Arts.

We may also collect personal information from third parties such as our related agencies, other grant funding applicants, credit reporting agencies, your representatives or publically available sources of information. All personal information that we collect is reasonably necessary for the purposes and functions of the Australia Council. These include:

- providing our services and fulfilling our functions under the *Australia Council Act 2013* (Cth) in supporting and promoting the arts;
- keeping you informed of relevant upcoming events, grants, funding initiatives and outcomes as well as our activities in general;
- improving our website and other services;
- conducting research into and about the arts and the programs we administer;
- to market our services, develop and identify new projects and conduct fundraising;
- evaluating the programs, support and funding we provide, including via surveys and interaction with recipients of our services;
- allowing the functions and services offered on the website to be provided to you; and
- complying with our legal obligations.

If we receive personal information about you that we did not ask for, from someone other than you, and we determine that we could have collected this information from you had we asked for it, we will notify you, as soon as practicable, that we have collected your personal information. If we could not have collected this personal information, we will lawfully de-identify or destroy that personal information.

We will not collect any sensitive information from you, revealing your race, ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships or details of health or disability. Exceptions to this include:

- where you have given express consent to us to do so and the information is reasonably necessary for us to provide our services or otherwise carry out our functions or activities;

- the use of this information is required or authorised under Australian law or a court or tribunal order; or
- when the information is necessary for the establishment, exercise or defence of a legal claim.

We will not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of our functions or activities. If we are unable to collect personal information we reasonably require, we may not be able to do business with you or the organisation with which you are connected.

To the extent you provide us with any personal information about another individual, you warrant that you are authorised to provide us with that information for use in accordance with this Privacy Policy.

COOKIES

When you visit our website the server may attach a "cookie" to the memory of your computer or device. A “cookie” assists us to store information on how visitors to our website use it and the pages that may be of most interest. This information may be used to make assumptions about who uses your computer or device and to provide users of your computer or device with information that we think may interest the users of your computer or device. You should be able to configure your computer or device so that it disables “cookies” or does not accept them if you wish. However, this information is not linked to any personal information you may provide and will not be used to identify you.

USE AND DISCLOSURE OF INFORMATION

We may use personal information about you for the primary purpose of providing you with our services, and which you would reasonably expect us to use that information for. This could include sending you information about new initiatives and programs, grant funding, our services or special events. We may send this information via post, telephone or any form of electronic communication. We may use any email address or other personal information you provide to us at any time for this purpose.

We will not disclose information that personally identifies you to any third party other than as set out in this Privacy Policy. In order to deliver the services that we provide to you, we may disclose your personal information to our related agencies, third party service providers, suppliers and other organisations outside of us, only in relation to providing our services to you. We take reasonable steps to ensure that these organisations are bound by privacy obligations in relation to the protection of your personal information.

In the event of a security incident involving unauthorised access, use or disclosure of personal information where a third party with whom we share personal information is involved, we will seek to work cooperatively with them to protect the personal information we have shared with them.

DIRECT MARKETING

We may use personal information about you for the primary purpose of providing you with information about our services, and which you would reasonably expect us to use that information for. This could include sending you information about new initiatives and programs, grant funding, our services or special events. We may send this information via post, telephone or any form of electronic communication. We may use any email address or other personal information you provide to us at any time for this purpose.

You can, at any time, opt out of receiving marketing material by contacting our Privacy Officer. You agree and acknowledge that even if you opt out of receiving marketing material, we will still send you essential information that we are legally required to send you relating to the services we provide. Once you opt out of receiving marketing material from us, you agree and acknowledge that this removal from our distribution lists may take several business days after the date of your request to be removed.

ACCURACY OF YOUR INFORMATION

All reasonable steps are taken by us to ensure that your personal information held by us is accurate, up-to-date, complete, relevant and not misleading. If you believe that any of your personal information is not accurate, not up-to-date, incomplete, irrelevant or is misleading, please contact our Privacy Officer and we will take all reasonable steps to correct it within a reasonable time.

THIRD PARTIES AND YOUR INFORMATION

We will only collect, store, use or disclose information that personally identifies you as set out in this Privacy Policy unless we are required to protect our rights or property (or those of any third party), or to avoid injury to any person, by law.

Although our website may link directly to websites operated by third parties (**Linked Sites**), you acknowledge that Linked Sites are not operated by us. We encourage you to always read the applicable privacy statement or policy of any Linked Site on entering the Linked Site. We are not responsible for the content or practices of the Linked Sites nor their privacy policies regarding the collection, storage, use and disclose of your personal information.

DISCLOSURE OF INFORMATION OVERSEAS

From time to time we may transfer any of your personal information to people in foreign countries to fulfil the purposes and functions of the Australia Council for the Arts.

An example would be where we are required to pass the shortlist of applications in a particular grant round to an overseas third party to assist us in making the final funding decision (e.g. an overseas studio residency program).

In many cases the transfer will be necessary for the performance of our contract with you or for the implementation of measures taken in response to a request by you or for the performance of a contract with a third party which is included in your interests.

Unless you advise us that you do not agree to this transfer it will be understood that when you apply for that particular grant round, you have agreed and consented to this transfer if and when it is necessary and in order for us to perform our functions. You acknowledge that where information is disclosed to an overseas recipient, they may not be subject to the Privacy Act.

YOUR CONSENT

By your use of our website you consent to the collection, storage, use and disclosure of your personal information in accordance with this Privacy Policy and as otherwise permitted under the Privacy Law.

STORAGE AND SECURITY

The Australia Council stores personal information in a variety of ways including email, electronic databases, electronic record management systems and cloud-based software.

We will use all reasonable endeavours to keep your personal information in a secure environment, by employing appropriate technical, administrative and physical procedures. These measures are designed to assist in your personal information not being accessed by unauthorised personnel, or from being lost or misused. If you reasonably believe that there has been unauthorised use or disclosure of your personal information please contact our Privacy Officer.

If we no longer need your personal information, unless we are required by law or a court or tribunal order to retain it, we will take reasonable steps to destroy or de-identify your personal information.

Notwithstanding the reasonable steps taken to keep information secure, breaches may occur. In the event of a security incident we have in place procedures to promptly investigate the incident and determine if there has been a data breach involving personal information, and if so, to assess if it is a breach that would require notification. If it is, we will notify affected parties in accordance with Privacy Law requirements.

VARIATION AND CONSENT TO VARIATION

We may at any time vary the terms of this Privacy Policy. You should check this Privacy Policy regularly so that you are aware of any variations made. You will be deemed to have consented to such variations by your continued use of our website following such changes being made.

ACCESS TO INFORMATION WE HOLD ABOUT YOU

If you request access to the personal information we hold about you, we will respond to your request within a reasonable period of time and, where reasonable and practicable, give access to the information in the manner you request. This will be subject to any exemptions allowed under the Privacy Law.

You have the option to either not identify yourself or to use a pseudonym when you contact us, unless it is impracticable for us to communicate with you in that manner or unless we are required or authorised under law, or a court or tribunal order, to deal with individuals who have identified themselves.

PERSONS LOCATED IN THE EU

If you are located in the EU, the General Data Protection Regulation (EU) 2016/679 (**GDPR**) provides for additional rights in relation to your personal information that we process. We take these rights into account when processing your personal information, including:

- **Erasure**: You have the right to request that we delete personal information we hold about you in certain circumstances, including where the information is no longer required.
- **Objection**: Depending on the circumstances in which we collected your personal information, you may have the right to object to our processing of your personal information.
- **Portability**: Depending on the circumstances, you have the right to receive and have transmitted to other data controllers any personal information we hold in a commonly used and machine-readable format, where technically feasible.
- **Restriction**: You have the right to restrict our processing of your personal information in certain circumstances, including where the accuracy of the information is contested, the processing is unlawful or the information is no longer required.
- **Review**: Unless necessary for the purpose of performing a contract between us, authorised by law or otherwise explicitly consented to by you, you can exercise your right not to be subject to decisions based on automated processing (such as online profiling).
- **Withdrawal**: Where we process your personal information based on your consent, you have a right to withdraw that consent at any time. You can withdraw consent by contacting our Privacy Officer or EU Representative, whose details are set out at the end of this Policy.

These rights are subject to certain restrictions and exemptions under Privacy Laws.

Whenever we collect your personal information, we will endeavour to obtain your consent to process your information for the purposes outlined in this Privacy Policy. We rely on this consent as the lawful basis to process your information, however, under GDPR, we may also process your information if the processing is necessary for:

– the performance of, or entering into, a contract with you;
– compliance with our legal obligations;
– protecting the vital interests of an individual;
– performing a task in the public interest; or
– the purposes of legitimate interests pursued by us or a third party.

CONTACT US

If you have any questions or wish to access or correct personal information, or are otherwise seeking to exercise your rights in respect of your personal information held by us, please contact us in writing:

The Privacy Officer
Australia Council for the Arts
372 Elizabeth Street
Surry Hills NSW 2010

or by sending an email to us at privacyofficer@australiacouncil.gov.au

If you contact us and are not satisfied with our response, you can may make a complaint to:

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

or by sending an email to enquiries@oaic.gov.au.

ANNEXURE 1:

NOTIFIABLE DATA BREACHES – POLICY AND RESPONSE PLAN

1. PURPOSE

The purpose of this annexure to the Privacy Policy is to ensure there are clear procedures in place for the management and notification of data breaches in order to comply with the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (an amendment to the *Privacy Act 1988*) effective 22 February 2018.

2. POLICY STATEMENT

The Australia Council is committed to ensuring an environment with clear procedures and processes for privacy data breaches. The Australia Council has obligations under the *Privacy Act 1988* (Cth) (**Privacy Act**) to put in place reasonable security safeguards and to take active steps to protect the personal information that it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

3. SCOPE

This policy applies to all "officials"[1] of the Australia Council including, but not limited to, employees, independent contractors, Board members, peers and agents. It also applies to third party suppliers and contractors who provide services to the Australia Council.

4. NOTIFIABLE DATA BREACHES

The Australia Council is required to comply with the Privacy Act. The Notifiable Data Breach scheme obliges all organisations required to comply with the Privacy Act to notify any individuals likely to be at risk of serious harm by a data breach.

What is a notifiable data breach?

A Notifiable Data Breach is **a data breach that is likely to result in serious harm** to any of the individuals to whom the information relates.

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. Examples of a data breach include when:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

[1] Refer to Section 13 of the *Public Governance, Performance and Accountability Act 2013*

What is "serious harm"?

"Serious harm" is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm. Whether a data breach is "likely to result" in serious harm to an individual whose information was part of the data breach requires an objective assessment from the perspective of a reasonable person. Under this scheme a "reasonable person" means a person in the entity's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available and/or following reasonable inquiries or an assessment of the data breach.

The phrase "likely to result" means the risk of serious harm to an individual is more probable than not (rather than possible).

In assessing whether a data breach is "likely to result" in serious harm the following needs to be considered:

- the type or types of personal information involved in the data breach;
- the circumstances of the data breach; and
- the nature of the harm that may result from the data breach.

Assessing the degree of harm caused as a result of a data breach – and whether the data breach is notifiable – will be undertaken by the Data Breach Response Team.

5. RESPONSE TO DATA BREACHES

The Australia Council has a robust approach to protection of personal information and this is reflected in our Incident Response Plan at **Attachment 1** and Incident Reporting Plan at **Attachment 2**.

We are committed to following this policy and the Incident Response Plan for a number of reasons including:

- mandatory compliance with the *Privacy Act*;
- maintaining the protection of the personal information of all stakeholders; and
- instilling public confidence in our capacity to protect personal information as well as responding appropriately to a data breach.

6. DATA BREACH RESPONSE TEAM

The Data Breach Response Team is comprised of the individuals across relevant Business Units at the Australia Council who are best placed to determine the response to a potential data breach. The Data Breach Response Team will be coordinated by General Counsel but at a minimum, the team includes:

- General Counsel, Corporate Resources
- I.T. Manager, Corporate Resources
- Director, Communications

- Executive Director (of the team with the relevant breach)

7. ROLES AND RESPONSIBILITIES

This section outlines the responsibilities of management and staff in relation to notifiable data breaches. (*Refer to Attachments 1 and 2*)

Role	Responsibility
All Staff	Escalate a data breach, or suspected data breach, to their Manager (or their relevant Executive Director if their Manager is unavailable) as soon as it becomes known
Manager, Business Unit	Escalate the data breach, or suspected data breach, to Legal and Governance and I.T. and the relevant Executive Director if not already done so
I.T.	Contain (if possible) the breach and prevent additional information loss; start forensic examination into the source, and extent, of the breach; implement measures to prevent a further data breach; liaise with third party I.T. providers as required
Legal and Governance	Assess the extent and cause of the breach and any potential serious harm to any individual(s); determine which individuals and (possible) organisations are required to be notified; consider any legal or contractual obligations that may arise; determine whether the matter needs to be escalated to the Data Breach Response Team and/or recommend the overall response action to be taken to the Executive
Communications	Liaise with I.T. and Legal and Governance to determine the extent of the breach; assist to prepare statements for the OAIC, affected individuals and (possible) organisations, media and the website; consider whether further contact options, including a dedicated telephone line, will be required for affected individuals
Finance	Determine whether the Australia Council's insurer needs to be put on notice
Executive Director	Brief the CEO and/or Director Communications where appropriate; liaise with Legal and Governance on response action to be taken and whether the Data Breach Response Team needs to be convened

Data Breach Response Team	Assess and contain the breach as soon as possible; notify the individual(s) affected if required; notify any relevant organisations if appropriate; notify the Office of the Information Commissioner if required
CEO	Ensure the Australia Council has an appropriate policy and response plan in place to comply with the Privacy Act

8. DEFINITIONS

Australian Privacy Principles means the principles under the *Privacy Act 1988* by which relevant entities, including the Australia Council, must use, handle and manage personal information.

GDPR means the General Data Protection Regulation 2016/679 which is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.

Notifiable Data Breach means a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. It occurs when personal information held by the Australia Council is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

OAIC means the Office of the Australian Information Commissioner

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

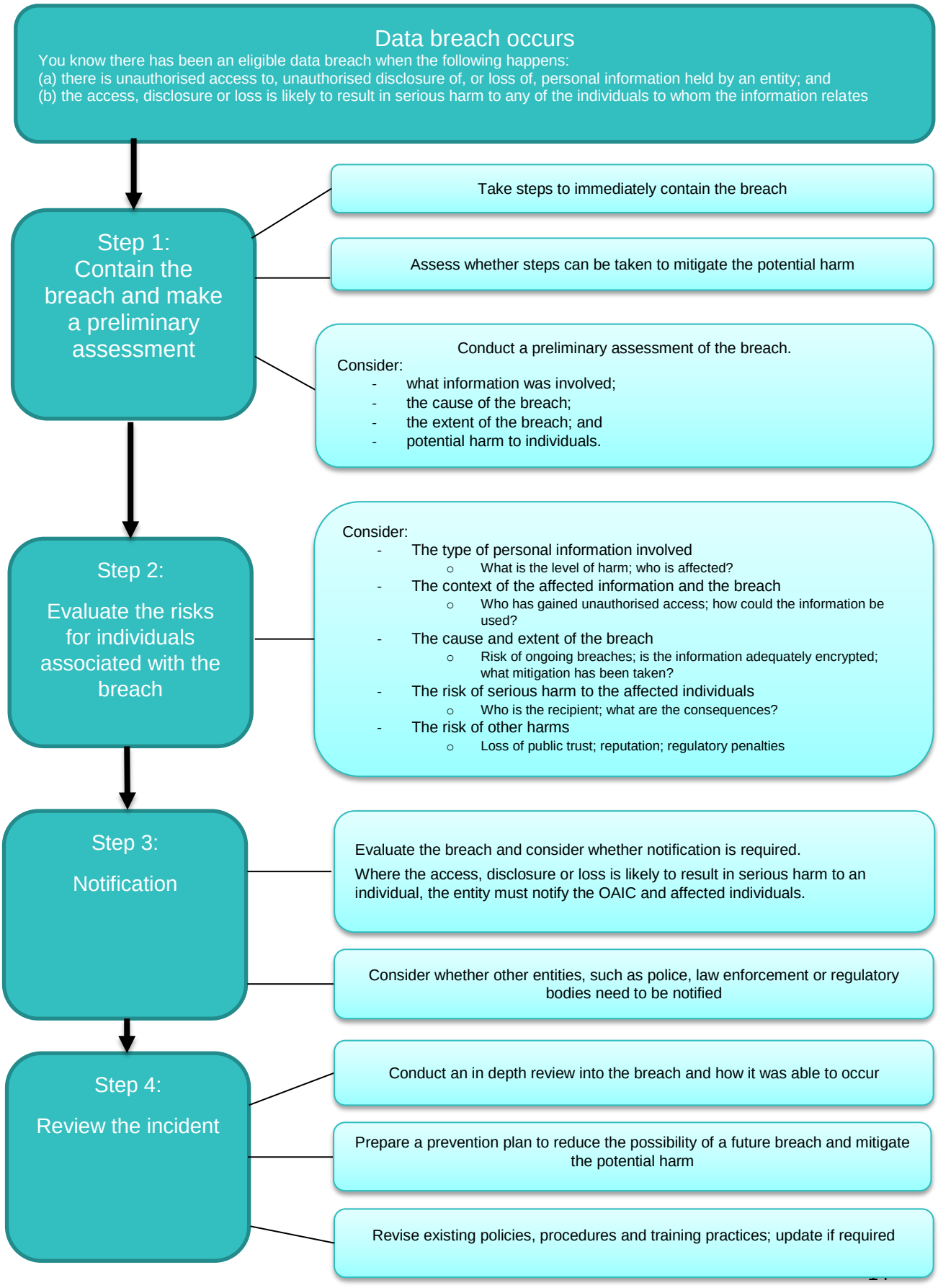
- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

9. INTERACTING POLICIES AND LEGISLATION

This policy should be read in conjunction with:

- *Archives Act 1983* (Cth)
- Australia Council Privacy checklist
- Privacy Act 1988 (Cth)
- Public Governance Performance and Accountability Act 2013 (Cth)
- The Australian Government Agencies Privacy Code
- The General Data Protection Regulation (EU) 2016/679

Attachment 1: Incident Response Plan



Attachment 2: Incident Reporting Plan

When a data breach has occurred or is suspected to have occurred

Staff member:

- Immediately notify Manager of the breach (or Executive Director if Manager unavailable)
- Record and advise:
  - The time and date of discovery;
  - The type of personal information involved;
  - Cause and extent of the breach; and
  - The context of the affected information

Manager:

- Consider whether immediate action can reduce further loss or mitigate damage; and
- Escalate the data breach, or suspected data breach, to Legal and Governance and the relevant Executive Director.

Relevant business units including I.T. and Legal & Governance:

- Work together to contain the breach, determine the extent of the breach and any associated risks; and
- Work with the Executive Director to determine response action to be taken.

Executive Director:

- Brief the CEO; and
- Work with Legal and Governance and the relevant Business Units to formulate response action to be taken and determine whether the Data Breach Response Team needs to be convened

Data Breach Response Team:

- Convene with the relevant Business Units to investigate the breach;
- Assess the severity of the breach(es) and
- Take the appropriate action as required under the Privacy Act.

Attachment 3: Does the GDPR apply? If yes, see Article 33 below

Notification of a personal data breach to the supervisory authority

In the case of a personal data breach:

- the **controller** shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
- The **processor** shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification shall at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay

The **controller** shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article. If the breach is likely to result in high risk to the individual then under Article 34 it must be notified to the individual in accordance with Article 34.

CHANGE HISTORY

Date	Change Description	Reason for Change	Author	Issue No:
March 2014	Initial document creation	Amendment to the *Privacy Act 1988* and introduction of the Australian Privacy Principles	Rebecca Kenny	1.0
August 2014	Updated	Updated to reflect new branding and style guide	Rebecca Kenny	2.0
June 2016	Review	Scheduled two year review and update (no changes)	Rebecca Kenny	2.1
December 2017	Updated	Updated to comply with the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (commencement date; 22 February 2018)	Rebecca Kenny	3.0
Sept 2018	Updated	Updated to clarify purpose, collection and handling processes for personal information under the Privacy Code (commenced on 1 July 2018) and to incorporate the General Data Protection Regulation (EU) (commenced on 25 May 2018)	Rebecca Kenny	4.0