PRIVACY POLICY

Issue No:	4.2
Dated Issued:	March 2014
Reviewed:	February 2020
Next Review Date:	February 2022
Document Status:	FINAL
Prepared by:	Rebecca Kenny, General Counsel
Approved by:	The Executive (September 2018)

CONTENTS

INTRODUCTION

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

This Privacy Policy has been developed in accordance with the Commonwealth *Privacy Act 1988* (**Privacy Act**), the *Privacy Amendment (Notifiable Data Breaches) Act 2017* and the Australian Government Agencies Privacy Code (**Privacy Code**). 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**). Collectively we refer to the above legislation as the "**Privacy Laws**".

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 Laws, 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.

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.

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

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 publicly 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;
- marketing our services, developing and identifying new projects and conducting 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 for us to do so and the information is reasonably necessary for us to provide our services to you 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 Laws.

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 at: privacyofficer@australiacouncil.gov.au.

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 and, where reasonable and practicable, give access to the information in the manner you request. This will be subject to any requirements under the Privacy Laws.

ANONYMITY AND PSEUDONYMITY

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 the 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.

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 (refer Attachment 1) 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.

INTERACTING POLICIES AND LEGISLATION

This policy should be read in conjunction with:

- *Privacy Act 1988* (Cth)
- *Privacy Amendment (Notifiable Data Breaches) Act 2017*
- The Australian Government Agencies Privacy Code
- The General Data Protection Regulation (EU) 2016/679
- *Public Governance Performance and Accountability Act 2013* (Cth)
- *Archives Act 1983* (Cth)

CONTACTING 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
Level 5
60 Union Street
Pyrmont NSW 2009

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:

AUSTRALIAN PRIVACY PRINCIPLES (APPS)[2]

Overview of the Australian Privacy Principles

Overview

This Schedule sets out the Australian Privacy Principles.

Part 1 sets out principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.

Part 2 sets out principles that deal with the collection of personal information including unsolicited personal information.

Part 3 sets out principles about how APP entities deal with personal information and government related identifiers. The Part includes principles about the use and disclosure of personal information and those identifiers.

Part 4 sets out principles about the integrity of personal information. The Part includes principles about the quality and security of personal information.

Part 5 sets out principles that deal with requests for access to, and the correction of, personal information.

Australian Privacy Principles

The Australian Privacy Principles are:

- Australian Privacy Principle 1—open and transparent management of personal information
- Australian Privacy Principle 2—anonymity and pseudonymity
- Australian Privacy Principle 3—collection of solicited personal information
- Australian Privacy Principle 4—dealing with unsolicited personal information
- Australian Privacy Principle 5—notification of the collection of personal information
- Australian Privacy Principle 6—use or disclosure of personal information
- Australian Privacy Principle 7—direct marketing
- Australian Privacy Principle 8—cross border disclosure of personal information
- Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers
- Australian Privacy Principle 10—quality of personal information
- Australian Privacy Principle 11—security of personal information
- Australian Privacy Principle 12—access to personal information
- Australian Privacy Principle 13—correction of personal information

[2] Schedule 1, Privacy Act 1988

Part 1—Consideration of personal information privacy

1 Australian Privacy Principle 1—open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

2 Australian Privacy Principle 2—anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Part 2—Collection of personal information

3 Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

4 Australian Privacy Principle 4—dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

5 Australian Privacy Principle 5—notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Part 3—Dealing with personal information

6 Australian Privacy Principle 6—use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

7 Australian Privacy Principle 7—direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual’s attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception—sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception—contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(aa) Division 5 of Part 7B of the *Interactive Gambling Act 2001*;

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

8 Australian Privacy Principle 8—cross border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For permitted general situation, see section 16A.

9 Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For permitted general situation, see section 16A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Part 4—Integrity of personal information

10 Australian Privacy Principle 10—quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up to date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

11 Australian Privacy Principle 11—security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de identified.

Part 5—Access to, and correction of, personal information

12 Australian Privacy Principle 12—access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

13 Australian Privacy Principle 13—correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

ANNEXURE 2:

NOTIFIABLE DATA BREACHES – POLICY AND RESPONSE PLAN

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.

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.

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.

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 potential degree of serious harm caused as a result of a data breach – and whether the data breach is notifiable – will be undertaken by General Counsel in the first instance or the Data Breach Response Team if convened.

RESPONSE TO DATA BREACHES

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

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 responsible for the relevant breach)

ROLES AND RESPONSIBILITIES

This section outlines the responsibilities of Council Officials in relation to potential or actual notifiable data breaches. (*Refer to Attachments 1 and 2*)

Role	Responsibility
Council Officials	Escalate a data breach, or suspected data breach, to their Manager (or their relevant Executive Director if their Manager is unavailable) and Legal and Governance 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
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; consider whether the Data Breach Response Team needs to be convened 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 determine 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 Laws

Attachment 1: Incident Reporting Plan

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

Council Official:

- Immediately notify Manager (or Executive Director if Manager unavailable) or Council contact of the breach
- 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.

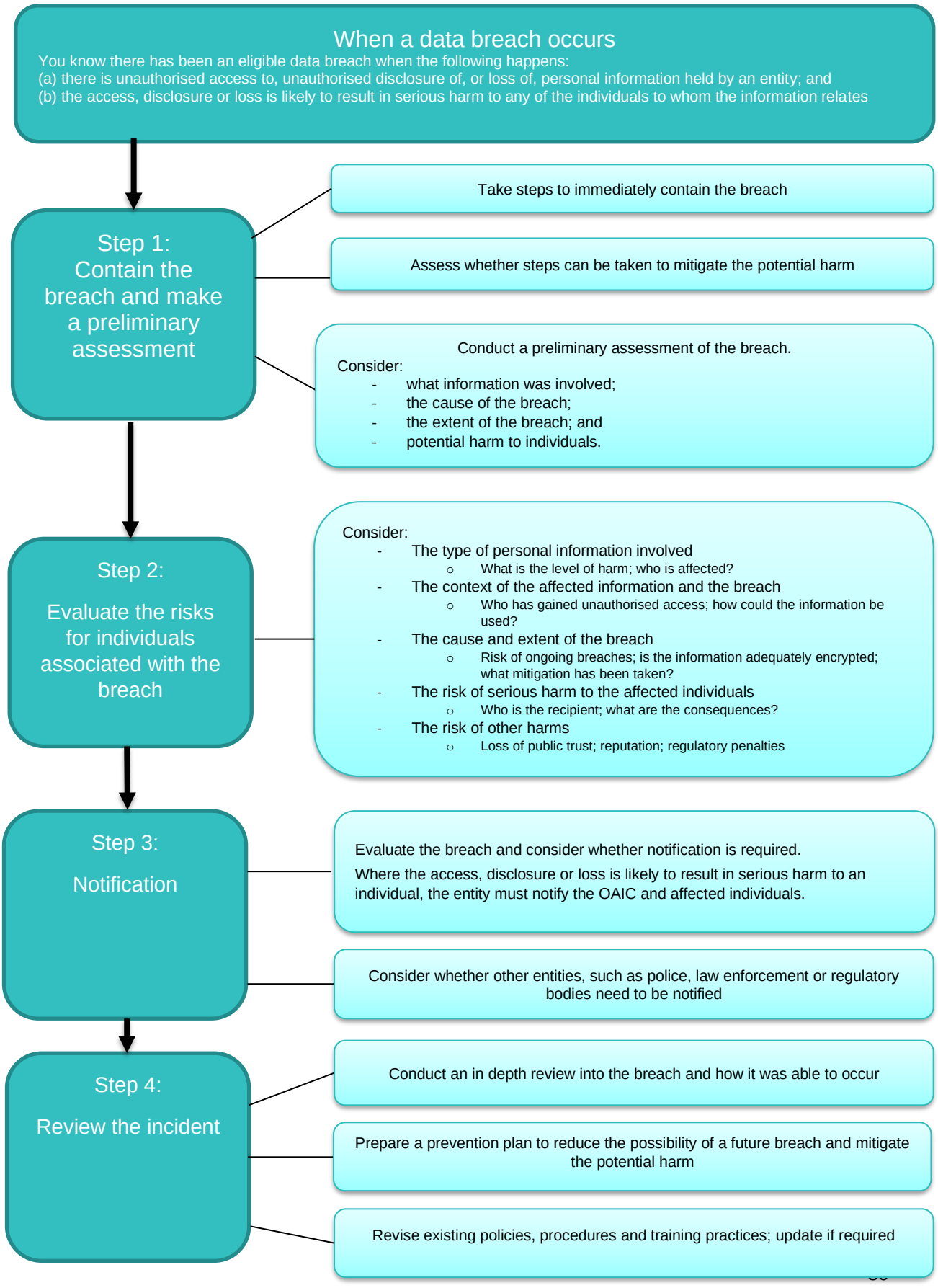
Executive Director:

- 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 2: Incident Response Plan



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
December 2019	Updated	Minor updates for further clarification and due to office relocation	Rebecca Kenny	4.1
February 2020	Updated	Updated to include APPs as per internal audit recommendation	Rebecca Kenny	4.2