



P16 – Privacy Policy

January 2020

cancercouncil.com.au

Contents

1.	Introduction	3
2.	Application and review.....	3
3.	Definitions.....	3
4.	Collection of Personal Information.....	4
5.	Use of Personal Information.....	6
6.	Disclosure.....	9
7.	Data Security	10
8.	Access and Correction.....	11
9.	Complaints	12
10.	References / related documents	12

1. Introduction

- 1.1 Cancer Council NSW (Cancer Council) recognises the importance the community places on the maintenance of privacy of individuals' personal and/or sensitive information. As an "APP entity" (as defined under the *Privacy Act 1988 (Cth)*), Cancer Council is bound by the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles, as well as the *Health Records and Information Privacy Act 2002 (NSW)* which governs the handling of health information in NSW.
- 1.2 This Policy sets out Cancer Council's approach to the handling of individuals' Personal Information, including sensitive information and health information.
- 1.3 This policy may be reviewed and varied from time to time in accordance with the relevant legislation requirements and to meet the ongoing needs of the organisation.

2. Application and review

- 2.1 This policy was last updated in January 2020 and will be reviewed on or before January 2023. It replaces all other versions of this policy.
- 2.2 This policy applies to all Cancer Council workers, including casual employees and contractors, and volunteers. Non-compliance may result in disciplinary action, including termination of employment. Whilst they are required to comply with this policy, which may be updated and amended from time to time, it does not form part of any employee's contract of employment or other contract and does not create or confer any entitlement, legal right or enforceable benefit.

3. Definitions

- 3.1 In this policy:

APP means Australian Privacy Principle, as set out in the *Privacy Act 1988 (Cth)*.

Cross Border Disclosure means a disclosure of personal information to an entity that is located outside Australia

Disclosure means in relation to personal information, a release of that personal information from the effective control of Cancer Council, including but not limited to:

- (a) an automatic release, to a person or body that Cancer Council knows has a general authority to access that personal information; or
- (b) in response to a specific request.

Storage of personal information in the cloud may or may not constitute disclosure. Where the cloud solution is infrastructure-as-a-service (IAAS), the personal information stays in the effective control of Cancer Council and there is therefore no disclosure. Where the cloud solution is software-as-a-service (SAAS), a disclosure is likely to have occurred. If unsure, consult IT Operations.

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

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

Sensitive information is a subset of personal information, which is information or opinion about an individual's racial or ethnic origin, political opinions, membership of a

political organisation, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, health information genetic information, biometric information and biometric templates.

Supporter means an individual or organisation who has donated money, goods or services, or participated in fundraising activities in support of Cancer Council or has participated in a research study or is a volunteer.

Use means, in relation to personal information, any accessing by an agency of personal information in its control, including searching records for any reason, using personal information in a record to make a decision and passing a record from one part of the organisation to another part.

Worker means any Cancer Council employee (including casual employees), contractors and volunteers

4. Collection of Personal Information

4.1 General Principle

Workers should only collect personal information about individuals where the collection is reasonably necessary for one or more of Cancer Council's functions or activities.

4.2 Types of information collected

Cancer Council collects personal information from people who are connected to its operations and activities, including workers, donors, event participants, research study participants, recipients of support services, participants in advocacy campaigns or health promotion projects, health professionals, suppliers, volunteers and service providers.

Where relevant to current business operations, workers are authorised to collect all types of personal information, including:

- contact information (both home and work) such as full name (first and last), email address, current postal address and phone numbers,
- date of birth,
- employment details, including but not limited to job title, training and skills,
- financial details, including insurance policies and details, if applicable,
- opinions via surveys and questionnaires, if applicable,
- details relating to goods and services,
- details relating to donations made,
- any relevant payment or billing information (including bank account details, credit card details, billing address and invoice details),
- usernames and passwords when setting up an account on our website, and
- health information and other relevant sensitive information.

4.3 Collection method

Where possible, workers should collect personal information directly from the individual. However, it is permissible to obtain personal information from third parties such as contractors (including fundraising service providers), list vendors, health professionals, social and community workers where necessary.

If personal information about an individual is collected from a third party and it is unclear that the individual has consented to the disclosure of his or her personal information to Cancer Council, workers should take reasonable steps to contact the individual and ensure that he or she is aware of the collection. In most cases, this can take place simultaneously with the first use of the information by Cancer Council. Workers should consult with the General Counsel if they are unsure whether it is reasonable in the circumstances to contact individuals to advise them of the collection of personal information.

Research studies with ethics approval from an Australian Human Research Ethics Committee (HREC) may have additional obligations in relation to collection of personal information. Workers involved in such projects must comply with the conditions of the ethics approval by the relevant HREC. In particular, collection of health information from health professionals and health record databases must be provided for in a peer-reviewed protocol that is approved by the relevant HREC, and consent must be obtained from the relevant individuals.

4.4 Collection notices

Where Cancer Council collects personal information (including sensitive information) from an individual, that individual should be provided with a collection notice. The collection notice should be drafted and/or approved by the General Counsel and should cover as many of the following matters as is reasonably practicable in the circumstances:

- Cancer Council's name and contact details,
- if the personal information was collected from someone other than the individual, how it was collected,
- whether the collection is authorised or required by law (if applicable),
- the purposes for which the information is being collected,
- the consequences to the individual of not providing the information,
- to whom Cancer Council usually discloses that kind of personal information,
- information about how to find or obtain our Privacy Policy, as well as information on access to and correction of personal information and how an individual may complain about a breach of the Australian Privacy Principles, and
- whether Cancer Council is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

Collection notices should generally be provided at the time the information is collected, by the worker responsible for collecting the information. Where this is not practical (for example, where information is collected from a third party), the collection notice should be provided at the time of first contact with the individual, by the worker responsible for making that first contact.

4.5 Collection by third parties as agent for Cancer Council

Where personal information is collected by third parties as agent for Cancer Council (for example, social workers collecting information for referral to support services, or fundraising services suppliers collecting information for direct marketing):

- wherever possible, our agent should provide Cancer Council's standard collection notice. Where Cancer Council has a contractual relationship with the agent or service provider, this requirement should be included, and
- where the third party does not show Cancer Council's collection notice to the individual, a collection notice must be provided by Cancer Council at the time

of the first use of the information (that is, the first contact with the individual by Cancer Council).

4.6 Sensitive information

In general, workers should attempt to limit the collection of sensitive information from individuals. However, sensitive information may need to be collected in order to deliver certain services, including information and support programs, or to conduct research studies. Workers should only collect sensitive information from or about an individual if it is necessary to deliver a service to that individual, or to conduct research according to an approved research protocol.

4.7 Anonymity

Where practicable, individuals should be given the opportunity to engage with Cancer Council on an anonymous basis or using a pseudonym. This requirement will rarely be applicable to individuals engaging with Cancer Council for the purpose of receiving our services and/ or participating in our programs, however, it may apply where an individual is contacting Cancer Council merely to obtain information. If an individual makes this request, and Cancer Council does not need his or her personal information to engage with the individual and/or provide the information requested, it should not be collected.

If possible, individuals should be advised of any consequences of not providing personal information to Cancer Council – for example, the fact that Cancer Council may not be able to deliver services to them effectively.

4.8 Unsolicited personal information

Where an individual provides personal information that has not been solicited by Cancer Council, the worker who receives that information should determine whether it is reasonably necessary for one or more of Cancer Council's functions or activities. If it is not, the information should be destroyed as soon as is practicable.

4.9 Website usage information and cookies

When individuals access Cancer Council's main website and certain other websites under the control of Cancer Council, the organisation may use software embedded in its website (such as Javascript) and may place small data files (or cookies) on the individual's computer or other device. The purpose of these cookies is to collect information about which pages they view and how they reach them, what they do when they visit a page, the length of time they remain on the page, and how Cancer Council performs in providing content to them. This also helps Cancer Council to serve the individual more efficiently if they revisit the site.

Cancer Council's website may use Google Analytics features, which tracks internet usage and discloses this to other members of the Google Ad network. Individuals can also opt out of Google Analytics by clicking on [Ad Settings](#).

Cancer Council does not currently associate such information with an identifiable person, and as such, the information so collected is not personal information.

5. Use of Personal Information

5.1 Use for primary and Secondary purposes

Workers must only use individuals' personal information for the primary purpose for which it was collected, a secondary purpose to which the individual has consented, or:

- for a purpose related to the primary purpose of collection and the individual would reasonably expect the personal information to be used for such a purpose
- where the worker, where practicable in consultation with the General Counsel, reasonably believes that the use is necessary to lessen or prevent a serious or imminent threat to an individual's life, health or safety or to lessen or prevent a threat to public health or safety, or
- where the worker, in consultation with the General Counsel, has reason to suspect that unlawful activity has been, or is being, engaged in.

There are other circumstances in which the General Counsel may determine that personal information may be used for legal purposes (for example, in relation to legal claims and alternative dispute resolution). If a worker is unsure as to whether personal information can be used for a specific purpose, the worker should consult the General Counsel.

Primary purposes (and secondary purposes for which consent is required) should be set out in collection notices, and may include:

- marketing: to communicate with individuals about donations, products, services, campaigns, causes and events
- support services: to provide individuals with information and support services, and to evaluate and report on these services
- research: to conduct and/or fund research into cancer causes, as well as prevention, diagnosis, treatment and survivorship
- health promotion: to provide individuals with information about cancer risk factors, such as UV exposure, tobacco and obesity, and to seek their support for campaigns
- volunteering and other support: to enable individuals to assist us with volunteering, community fundraising, advocacy and other activities where we seek the community's assistance, and

- 5.2 other issues: communicating with individuals in relation to our operations, activities and objectives, to verify their identity, to improve and evaluate our programs and services and to comply with relevant laws. **Use of Information collected as part of approved research studies**

Research studies that have been approved by a Human Research Ethics Committee may have different obligations in relation to use of personal information, including health information. Those obligations will apply in addition to this Privacy Policy and workers should refer to the terms of the ethics approval prior to using personal information collected for research studies.

5.3 **Use for Direct Marketing General principles**

Workers may use individuals' personal information for direct marketing purposes, but only where:

- the direct marketing communication contains a prominent statement that the individual may opt out of receiving that type of communication, and
- the relevant individual has not made such a request.

5.4 Consent for direct marketing

Individuals whose personal information is collected using a collection notice that references this Privacy Policy are taken to consent to the use of their personal information for direct marketing purposes, unless they have specifically opted out.

5.5 Opting out of direct marketing

Email direct marketing communications should generally contain an 'unsubscribe' link that provides individuals with the opportunity to opt out of direct marketing communications. In other circumstances, individuals who do not wish to receive direct marketing communications from Cancer Council may contact Cancer Council NSW, Donor & Supporter Services Unit, PO Box 572, Kings Cross NSW 1349, 1300 780 113, feedback@nswcc.org.au to opt out.

Workers must take all necessary steps to opt such individuals out of direct marketing communications. Requests to opt out of direct marketing communications should be treated in the first instance as a request to opt out of the particular event or campaign to which the communication relates. However, individuals must be given the opportunity to contact Cancer Council (for example, by phone or by email to the feedback email above) to opt out of all direct marketing communications, across all programs, events and channels.

Individuals who have opted out of direct marketing may still receive administrative emails, such as reminders to bank funds raised, to assist Cancer Council to comply with its regulatory obligations.

5.6 Removal of opt-outs

Individuals who register for events, make a donation or otherwise provide their personal information for marketing-related purposes after they have previously opted out of direct marketing communications (and who do not at the time of re-connecting with Cancer Council advise that they wish to opt-out of direct marketing communications) should be taken to have 'opted in' once again and may receive direct marketing communications. However, all such direct marketing communications must give the individual the opportunity to opt out, as described above.

Where:

- it is unclear as to whether an individual has opted out of direct marketing communications, or
- an opt-out direction has endured for two years or more,

then a communication may be sent to that individual, provided it gives the individual the opportunity to opt out, as described above.

The opt-out procedures described above are subject to the *Spam Act 2003* (Spam Act) and the *Do Not Call Register Act 2006* (DNCR Act), which override these procedures, where applicable. If a worker is unsure as to the application of the opt-out procedures or the application of the Spam Act or DNCR Act, they should seek advice from the General Counsel.

5.7 Business-to-business relationships

Where an individual provides his or her business contact details (such as a business card), this should be treated as implied consent to be contacted for business

purposes, and no additional collection notice is required. However, the individual should not be contacted in relation to marketing activity in their individual capacity unless he or she has provided specific consent (whether by accepting the terms of this Privacy Policy, the privacy statement on our website, via a collection notice or otherwise).

6. Disclosure

6.1 Permitted Disclosure

Workers may disclose individuals' personal information where the disclosure is for the primary purpose for which the information was collected, a secondary purpose to which the individual has consented, or:

- for a purpose related to the primary purpose of collection and the individual would reasonably expect the personal information to be used or disclosed for such a purpose,
- where the worker, where practicable in consultation with the General Counsel, reasonably believes that the disclosure is necessary to lessen or prevent a serious or imminent threat to an individual's life, health or safety or to lessen or prevent a threat to public health or safety,
- where the worker, in consultation with the General Counsel, has reason to suspect that unlawful activity has been, or is being, engaged in, or

6.2 where disclosure is required or authorised by law. Usual Disclosures

Individuals whose personal information is collected using a collection notice that references this Privacy Policy are taken to consent to the following disclosures:

- external support services, including health care professionals, lawyers, other professionals, counsellors, funders, financiers, co-ordinators, volunteers, service providers, agencies and not-for-profits that provide support services,
- researchers and research institutions that conduct research studies to cancer causes, as well as prevention, diagnosis, treatment and survivorship,
- charitable and other similar organisations, including third party service providers who facilitate the sharing of information between such types of charitable or similar organisations (including data collectives),
- contractors and service providers who perform services on Cancer Council's behalf, such as mailing houses, printers, information technology services providers (including offshore cloud computing service providers), data matching and data washing service providers, database contractors and telemarketing agencies, and
- Cancer Council Australia and State and Territory Cancer Councils that are members of Cancer Council Australia

6.3 Disclosure of Information collected as part of approved research studies

Research studies that have been approved by a Human Research Ethics Committee may have different obligations in relation to disclosure of personal information, including health information. Those obligations will apply in addition to this Privacy Policy and workers should refer to the terms of the ethics approval prior to disclosing personal information collected for research studies.

6.4 Disclosure to other Cancer Councils

Where Cancer Council is collecting personal information from individuals on behalf of other Cancer Councils, workers must take reasonable steps to obtain consent from the relevant individuals for disclosure to those Cancer Councils. Workers should consult with the General Counsel if they are unsure whether it is reasonable in the circumstances to obtain consent from individuals in relation to this disclosure.

6.5 Cross-border disclosures

Cancer Council may use data hosting facilities or enter into contractual arrangements with third party service providers to assist it with providing our goods and services. As a result, personal information provided to Cancer Council may be transferred to, and stored at, a destination outside Australia, including but not limited to New Zealand, Netherlands, China, Singapore, Hong Kong, Ireland, Canada, United States of America and the United Kingdom.

Personal information may also be processed by staff or by other third parties operating outside Australia who work for Cancer Council or for one of its suppliers, agents, partners or other Cancer Councils.

For other collections, workers must take reasonable steps to ensure that individuals are made aware of any likely cross-border disclosures of personal information and consent to such disclosures. Workers should consult with the General Counsel if they are unsure what may be considered reasonable in the circumstances.

Individuals whose personal information is collected using a collection notice that references this Privacy Policy are taken to consent to the disclosure, transfer, storing or processing of their personal information outside of Australia in the circumstances described. These individuals understand and acknowledge that countries outside Australia do not always have the same privacy protection obligations as Australia in relation to personal information.

Where personal information has been collected as part of a research study conducted by Cancer Council, the terms of the relevant ethics approval will provide that workers may only disclose personal information to offshore entities that are required to comply with Australian privacy laws, or privacy laws that offer equivalent protection. Workers must comply with this standard.

7. Data Security

7.1 Maintaining security of personal information

Cancer Council will take reasonable steps to help ensure the security of personal information, including by:

- making sure that personal information is accurate, complete and up to date,
- protecting personal information from misuse, loss, unauthorised access, modification or disclosure both physically and through computer security methods, and
- destroying or permanently de-identifying personal information if it is no longer needed for any authorised purpose.

7.2 Responding to a Data Breach

Cancer Council has implemented a Data Breach Response Plan, a copy of which is available on Dougal, which sets out the roles and responsibilities of workers in managing an appropriate response to a data breach and the steps to be taken if a breach occurs. This is applicable where personal information held by Cancer Council

is lost or subjected to unauthorised access, modification, disclosure or other misuse or interference.

In summary (there are further details in the Data Response Plan), Cancer Council will:

- conduct an investigation quickly and efficiently to determine if the breach is likely to result in serious harm to an affected individual. That assessment must be undertaken within 30 days of becoming aware that there are reasonable grounds to suspect a data breach, and
- determine whether notification to the Office of the Australian Information Commissioner is required. If required, the General Counsel will notify the Office of the Australian Information Commissioner and will arrange notification to the affected individuals.

8. Access and Correction

8.1 Access

Individuals are entitled to access any personal information held by Cancer Council about them, except in some exceptional circumstances provided by law. Where an individual requests access to their personal information, workers should verify the individual's identity (for example, by asking the individual to confirm their name, address and date of birth) and subject to the exceptions described below, should provide the personal information requested. However, Cancer Council is not required to provide access to personal information where:

- access would pose a serious threat to the life, safety or health of any individual or to public health or public safety,
- access would have an unreasonable impact on the privacy of other individuals,
- the request is frivolous or vexatious,
- denying access is required or authorised by a law or a court or tribunal order,
- access would be unlawful, or
- access may prejudice commercial negotiations, legal proceedings, enforcement activities or appropriate action being taken in respect of a suspected unlawful activity or serious misconduct.

If there is an operational reason why the worker does not wish to provide the information or the request is not straightforward and the worker is unsure how to handle the request, the worker should seek advice from the General Counsel.

Participants in research studies should note that access to personal information such as DNA sequences is not generally granted. This is notified to participants where applicable, at the time of committing to the research study.

Cancer Council's policy is that all requests for access to personal information will be responded to within 20 to 30 days.

Any decision to refuse a request for personal information should be handled by the General Counsel. Cancer Council will provide the individual with a written notice setting out the reasons for the refusal or for why the request has been handled in a particular way and notify the individual about the complaint mechanisms available (see *Complaints* below).

8.2 Correction

Individuals are entitled to seek to have personal information about them corrected. If an individual makes such a request, workers should correct the information. However, if there is an operational reason why the worker does not wish to correct the information or the request is not straightforward and the worker is unsure how to handle the request, the worker should seek advice from the General Counsel.

Due to the complexity of Cancer Council's operations, individuals' personal information may be stored simultaneously in more than one database or location. Workers must use reasonable endeavours to update all known instances where a request for correction of personal information by an individual is able to be fulfilled.

Cancer Council's policy is to respond to requests for correction in a timely manner.

Any decision to refuse a request to correct personal information should be handled by the General Counsel. Cancer Council will provide the individual with a written notice setting out the reasons for the refusal or for why the request has been handled in a particular way and notify the individual about the complaint mechanism available (see *Complaints* below).

9. Complaints

9.1 Complaints handling

All individuals who have been refused access or refused correction (see above) or have been subject to some other decision by Cancer Council regarding their personal information with which they do not agree, must be advised of the complaints mechanisms available to the individual, as follows:

- a complaint should firstly be made in writing to the General Counsel of Cancer Council by email on privacy@nswcc.org.au, by telephone on (02) 9334 1417, or by post at 153 Dowling St Woolloomooloo NSW 2011,
- Cancer Council will respond in a timely manner and will generally respond within 30 days,
- the complaint may then be taken to an externally recognised dispute resolution scheme (if any), and
- lastly, a complaint may be made to the Information Commissioner.

It is the General Counsel's responsibility to handle all complaints and to determine whether the complaint concerns a breach of the APPs, a privacy law or other applicable law.

Cancer Council may also receive complaints from the Office of the Information Commissioner (OAIC) regarding privacy issues. Generally, the OAIC will contact Cancer Council in writing where such a complaint is made. The General Counsel is responsible for dealing with all communications with the OAIC, the Information Commissioner or the Privacy Commissioner. If an worker receives a complaint or other communication by the Information Commissioner, the Privacy Commissioner or by a member of the OAIC's personnel by telephone, the worker should merely take the name and contact details of the person and promptly provide written notification to the General Counsel.

10. References / related documents

10.1 P17 Data Breach Response Plan