Council Policy

Council policy title:	**Privacy and Data Protection Policy 2017**
Council policy owner:	Director Corporate Services
Adopted by:	Bayside City Council
Date adopted:	19 December 2017
Scheduled review:	December 2019
Document Reference:	DOC/17/252752

(Council Policy is a high level public statement formally resolved by Council, which clearly states Council's requirements, intent or position with regard to a particular matter or issue. It is not intended to be procedural in nature.)

1. Policy intent

The responsible handling of personal information is a key aspect of democratic governance and Council is strongly committed to ensuring that personal information received by the Council is collected and handled in a responsible manner that maintains the privacy of an individual.

Accordingly, Council demonstrates its commitment through implementing the Information Privacy Principles ("IPPs") in the *Privacy and Data Protection Act 2014 (Vic)* and the Health Privacy Principles ("HPPs") in the *Health Records Act 2001 (Vic).*

In fulfilling the objectives of the Privacy Principles, Council is mindful of the need to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal and health information.

2. Policy purpose

To meet the Information Privacy Principles (IPPs) and Health Privacy Principles (HPPs) in relation to managing and handling personal and health information within the organisation.

3. Scope

This policy applies to all employees, Councillors, contractors and volunteers of Bayside City Council.

This policy applies to all personal information and health information held by Council, including personal information sourced by Council from third parties, that is information, or an opinion about an individual, whose identity is apparent, or can be reasonable ascertained, from that information or opinion.

(03) 9599 4444
PO BOX 27 SANDRINGHAM VIC 3191
www.bayside.vic.gov.au

4. Glossary - Definitions and Abbreviations

Term	Meaning
Personal Information	Means information or an opinion about an individual who can be identified from the information, or whose identity can reasonably be ascertained from the information. The information can be recorded in any form and does need to be true. This includes information the Council has collected in any format including correspondence, in person, over the phone and via our various web sites, or information or an opinion that forms part of a database. However, where the information is health information, it need not be recorded and, where the individual has been dead for more than 30 years, the information is no longer considered to be personal information. Examples of personal information: Names; addresses; contact details; work addresses; signatures; attendance at meetings; and opinions (particularly where those opinions would identify the person). Personal information on a public register, in complaints records, in records of telephone calls, on building plans, in meeting minutes and many, many other types of records held by the Council.
Health Information	Includes information or an opinion about the physical, mental, psychological health of an individual, disability of an individual or a health service provided or to be provided to an individual where that information is also personal information. Health information includes other personal information that is collected to provide or in providing a health service. Examples of health information: The view of a maternal child health nurse on a database that a mother may have an illness, records held by Council of attendees at immunisation sessions, requests for home support to be provided to a person living in the municipality made by family members outside the municipality.
Health service	Means an activity that is intended or claimed to assess, maintain or improve the individual's health, to diagnose the individual's illness, injury or disability or to treat the individual's illness, injury or disability.
Information Privacy Principles (IPPs)	Means a set of principles established by the Privacy and Data Protection Act 2014 that regulate how organisations such as the Council collects, hold, manages, uses, discloses or transfers health information.
Heath Privacy Principles (HPPs)	Means a set of principles established by the Health Records Act 2001 that regulate how a Council when it is a health service provider collects, holds, managers, uses, discloses or transfers health information.

Sensitive Information	Council may also hold sensitive information in order to provide education, welfare and other services. Sensitive information is personal information that is information or an opinion about an individual's: • Race or ethnic origin; • Political opinions; • Membership of a political association; • Religious beliefs or affiliations; • Philosophical beliefs; • Membership of a professional trade association; • Membership of a trade union; • Sexual preferences or practice; • Criminal record
Public Registers	Documents that are held by Council and : • Are open to inspection by members of the public; • Contain information that a person or body was required or permitted by legislation to give the Council under an Act or regulation; and • Contain information that would be personal information if the document was not a generally available publication.

5. **Policy statement**

The Privacy Data and Protection At 2014 (Vic) replaced the Information Privacy Act 2000 (Vic) and this policy reflects the change to a single privacy and data protection framework with clear privacy standards.

Under this Act Council has an obligation to collect and handle personal information in accordance with the 10 Information Privacy Principles (IPPs) which are listed below and further detailed in attachment 1:

Privacy Principles

Bayside City Council will manage personal information and health information as outlined in the following principles:

Collection of Information (IPP1) (HHP1)

Bayside City Council will only collect personal information that is necessary for specific and legitimate functions of Council.

Bayside City Council will only collect health information that is necessary for specific and legitimate functions of Council, and following the additional collection requirements of the HHP.

Information will be collected by fair and lawful means, and not in an unreasonable intrusive way.

Where reasonable and practicable to do so, Council will collect personal and health information directly from the individual involved. However, Council reserves the right to collect personal and health information from third parties where the law or circumstances warrant it.

In most cases, Council will advise individuals of its privacy practices, including the purposes for which their information is being collected, and of those third parties to whom their information is usually disclosed etc. However, council reserves the right not to do so where permitted by law.

Sensitive information will only be collected where the individual has consented or collection is otherwise required or permitted by law.

Sensitive information will be treated with the utmost security and confidentiality and only used for the purpose for which it was collected.

Use and Disclosure of Information (IPP2) and (HPP2)

Bayside City Council will not use or disclose information about an individual other than for the primary purpose or other Council business related purpose for which it was collected, unless one of the following applies:

For personal information – it is for a related purpose that the individual would reasonable expect;

For sensitive and health information – It is for a directly related purpose that the individual would reasonable expect;

Data Quality (IPP3) and (HPP3)

Council will take reasonable steps to ensure that all personal, sensitive and health information collected, held, used and disclosed is accurate, complete and up to data, bearing in mind and relevant to its purpose, functions and activities.

Data Security and Retention (IPP4) and (HPP4)

Council will take reasonable steps to prevent misuse or loss or unauthorised access, modification or disclosure or personal and health information.

Personal and health information will be managed confidentially and securely and destroyed, de-identified or archived in accordance with Public Records Office (Victoria (PROV) standards.

Council will monitor and implement reasonable and appropriate technical advances or management processes, to provide an up to date ongoing safeguard for personal information.

Openness (IPP5) and (HPP5)

Bayside City Council Privacy and Data Protection Policy will be available on Bayside's website or at the Corporate Centre and branch libraries.

Access to and Correction of Information (IPP6) and (HPP6)

Individuals have a right to request access to any personal or health information held about them, and may request any incorrect information be corrected.

Council may decide not to allow access to personal information or health information in accordance with the exemptions contained within the Privacy and Data Protection and Health Records Acts.

The process for requesting the correction of personal and health information, ie: documents, is through a Freedom of Information application.

Unique identifiers (IPP7) and (HPP7)

Council will not assign, adopt, use, disclose or require unique health or other identifiers from individuals except for the course of conducting normal business or if allows or required by law.

Anonymity (IPP8) and (HPP8)

Council will, where it is lawful and practicable, give individuals the option of not identifying themselves when entering into transactions with Council.

Council will ensure that individuals are aware of all, if any, limitations to services if the information requested is not provided.

Transborder Data Flows (IPP9) and (HPP9)

Bayside City Council will only transfer personal or health information outside of Victoria in accordance with the provisions outlined in the Privacy and Data Protection and Health Records Acts.

Sensitive Information (IPP10)

Bayside City Council will not collect sensitive information unless an individual has consented or collection is required or permitted by law, or when necessary for research or statistical purposes as permitted under the Privacy and Data Protection Act.

Transfer or Closure of Health Service (HPP11)

Health Information relating to a discontinued Council Health Service will be managed in accordance with the Health Records Act.

Making information available to another Health Service Provider (HPP12)

Council's Health Services will provide health information to other health providers in accordance with the Health Records Act.

Complaints or enquiries concerning privacy
Complaints, in the first instance, may be directed to the Governance Manager. These complaints will be acknowledged within two business days and will be resolved as soon as possible.

The complaint must be received within six months from the tine the complainant first became aware of the misconduct and details of the complaint will be kept confidential at all times.
Alternatively, complaints can be directed to the Commissioner for Privacy and Data Protection, although the Commissioner can decline a complaint if the complainant has not first complained directly to Council.

The Commissioner for Privacy and Data Protection can be contacts as follow:

Level 6, 121 Exhibition Street
MELBOURNE VIC 3000
Email: enquiries@privacy.giv.gov.au

Privacy Collection Statements
A general statement outlining Council's position on the handling of personal information will be used at all points of collection and all outgoing correspondence that may request personal or health information. This will include Bayside's website, advertising material, standard forms and correspondence requestion personal or health information.

Forms collecting information that is to be used for a specific purpose will include a privacy statement on the form including the purpose of collection and that the information may be used for other Council related purposes.

Council's privacy statements will be published in the relevant publications (eg: forms websites), confirming Council's commitment to the personal information and health information privacy principles.

6. Monitoring, evaluation & review

Non-compliance with this policy will breach the Privacy and Data Protection Policy. The register of alleged breaches will be monitored and reported to the Audit Committee quarterly on Council performance pursuant to this policy, with a summary of the number of complaints received and outcomes reported in the Annual Report.

This policy will be reviewed bi-annually.

7. Roles & Responsibilities

The Chief Executive Officer is responsible for the appointment of Bayside City Council's Information Privacy Officer. The Governance Manager and Governance Coordinator act as Council's Information Privacy Officers.

Information Privacy Officer

The role of the Information Privacy Officer includes:

- Inform and educate Council officers of their obligations under the Privacy and Data Protection and Health Records Act and to handle difficult enquires, complaints or adjustments concerning personal or health information.
- Provide advice and guidance to staff on Privacy related matters.
- Respond to requests for access to and correction of personal information in consultation with Council Officers.
- Investigate privacy complaints in consultation with complainants and Council officers. Respond to complainants and conciliate where necessary.
- Keep a record of alleged breaches.
- Respond to requests for access to and correction of health information in accordance with the Freedom of Information Act 1982 (Vic) and the Health Records Act.
- Ensure Council's privacy statements are accurate and up to date including privacy related information published on Council's websites (internet/intranet).

For all queries or feedback regarding this policy. Please contact the Governance Manager or contact email privacy@bayside.vic.gov.au

8. Public Registers

The following public registers are among those currently maintained by Bayside City Council which may include personal information:

- Details of current allowances fixed for the Mayor and Councillors
- Details of senior officers' total salary packages for the current financial year and the previous financial year.
- Details of overseas or interstate travel (with the exception of interstate travel by land for less than 3 days) undertaken in an official capacity by Councillors or Council staff in the previous 12 months.
- Names of sitting Councillors and Council officers who were required to submit a return of interest during the financial year and the dates the returns were submitted.
- Submissions received from the public in accordance with Section 223 of the Local Government Act 1989 during the previous 12 months.
- Details of all property, finance and operating leases involving land, buildings, plant, computer equipment or vehicles, entered into by the Council as lessor or lessee.

- A list of donations and grants made by the Council during the financial year.
- Names of the organisations of which the Council was a member during the financial year.
- A list of contract valued at $100,000 (or such higher amount as fixed by the State government from time to time) which the Council entered into during the financial year without first engaging in a competitive process.
- Campaign Donation Returns received from candidates in the 2016 Bayside City Council elections.

9. Related documents

Legislation	*Victorian Privacy and Data Protection Act 2014* *Victorian Health Records Act 2001* *Freedom of Information Act 1982 (Vic)* *Victorian Charter of Human Rights and Responsibility Act 2006 (Vic)* *Local Government Act 1989 (Vic)*

Please note: This policy is current as at the date of approval. Refer to Council's website (www.bayside.vic.gov.au) to ensure this is the latest version.

Information Privacy Principles

IPP1 – Collection
Collect only personal information that is necessary for the performance of functions, for a pre-determined purpose. Collect lawfully, fairly and not unreasonably intrusively. Advise individuals that they can gain access to their personal information.

IPP2 – Use and Disclosure
Use and disclose personal information for the primary purpose for which it was collected, or a related purpose a person would reasonably expect; otherwise, use and disclosure can only occur with consent. There are exemptions to disclosure restrictions; eg: law enforcement, life threatening emergencies.

IPP3 – Data Quality
Make sure personal information is accurate, complete and up to date.

IPP4 – Data Security
Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. Personal information should be destroyed or de-identified when it is no longer needed. Destruction should be in accordance with disposal schedules of the Public Records Act 1973.

IPP5 – Openness
Document clearly expressed policies of the management of personal information and provide the policies to anyone who asks. Know where to find the policy. Know who your privacy contact person is. Make sure the policy is reviewed to reflect current practice.

IPP6 – Access and Correction
Individuals have a right to seek access to their personal information and make corrections. Most requests for access and correction are handled under the Victorian Freedom of Information Act 1982.

IPP7 - Unique Identifiers
A unique identifier is usually a number assigned to an individual in order to identify the person for the purpose of an organisation's operations, eg: tax file no, drivers licence number. Unique identifiers can facilitate data matching, and this can in turn diminish privacy. So this IPP limits the assignment adoption, and sharing of unique identifiers.

IPP8 - Anonymity
Agencies must give individuals the option of not identifying themselves when entering transactions, if that is lawful and feasible.

IPP9 – Transborder data flows
Personal information can only be transferred interstate or overseas if certain conditions are met. Consent in one condition. Another condition is that the destination must have privacy standards similar to Victoria's IPPs.

IPP10 – Sensitive information
Collection of sensitive information is tightly restricted. This includes information or opinion about an individual's: political views; religious beliefs; sexual preferences; membership of groups (eg: unions political groups); racial or ethnic origin; or criminal record.

Health Privacy Principles

IPP1 – Collection
Collect only personal information that is necessary for the performance of functions, for a pre-determined purpose. Collect lawfully, fairly and not unreasonably intrusively. Advise individuals that they can gain access to their personal information.

IPP2 – Use and Disclosure
Use and disclose personal information for the primary purpose for which it was collected, or a related purpose a person would reasonably expect; otherwise, use and disclosure can only occur with consent. There are exemptions to disclosure restrictions; eg: law enforcement, life threatening emergencies.

IPP3 – Data Quality
Make sure personal information is accurate, complete and up to date.

IPP4 – Data Security
Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure. Personal information should be destroyed or de-identified when it is no longer needed. Destruction should be in accordance with disposal schedules of the Public Records Act 1973.

IPP5 – Openness
Document clearly expressed policies of the management of personal information and provide the policies to anyone who asks. Know where to find the policy. Know who your privacy contact person is. Make sure the policy is reviewed to reflect current practice.

IPP6 – Access and Correction
Individuals have a right to seek access to their personal information and make corrections. Most requests for access and correction are handled under the Victorian Freedom of Information Act 1982.

IPP7 - Unique Identifiers
A unique identifier is usually a number assigned to an individual in order to identify the person for the purpose of an organisation's operations, eg: tax file no, drivers licence number. Unique identifiers can facilitate data matching, and this can in turn diminish privacy. So this IPP limits the assignment adoption, and sharing of unique identifiers.

IPP8 - Anonymity
Agencies must give individuals the option of not identifying themselves when entering transactions, if that is lawful and feasible.

IPP9 – Transborder data flows
Personal information can only be transferred interstate or overseas if certain conditions are met. Consent in one condition. Another condition is that the destination must have privacy standards similar to Victoria's IPPs.

IPP10 – Transfer/closure practice
If the practice or business of a health provider is sold or transferred or if the provided is deceased, steps must be taken to notify individuals who have received health services from the provider.

IPP11 – Making information available to another service provider
An individual can request that a service provider make information relating to them available to another service provider.