

**Privacy Policy**

2016 Version 1.2

**Contents**

1 Background 3

2 Policy Statement 3

3 Scope 3

4 Definitions 3

5 Information Privacy and Health Privacy Principles 4

5.1 Privacy Principle 1 - Collection of personal and health information 4

5.2 Privacy Principle 2 - Use and disclosure of information 5

5.3 Privacy Principle 3 - Data quality 5

5.4 Privacy Principle 4 - Data security and retention 5

5.5 Privacy Principle 5 - Openness 5

5.6 Privacy Principle 6 - Access and corrections 5

5.7 Privacy Principle 7 - Unique identifiers 6

5.8 Privacy Principle 8 - Anonymity 6

5.9 Privacy Principle 9 - Trans-border data flows 6

5.10 Privacy Principle 10 - Sensitive information 6

5.11 Health Privacy Principle 10 and 11 - Health service provider changes 7

6 External contractors 7

7 What to do if you believe your personal information has been mishandled 7

8 Staff training and awareness 7

9 Related documents 8

10 Changes and review 8

11 Further information 8

Appendix A - Information Privacy Principles (IPP's) 9

Appendix A - Health Privacy Principles (HPP's) 10

Document control 11

# Background

Since 1st July 2002, all Victorian Councils have been required to comply with the *Privacy and Data Protection Act 2014* (previously known as the *Information Privacy Act 2000*) and the *Health Records Act 2001*. The Privacy and Data Protection Act 2014 regulates the management, collection, use and disclosure of ‘personal information’ and ‘sensitive information’, whilst the Health Records Act 2001 regulates the management, collection and use and disclosure of ‘health information’.

# Policy Statement

Hobsons Bay City Council is strongly committed to protecting and preserving an individual’s right to privacy and to the responsible and fair handling of their personal, sensitive and health information. Council is committed to full compliance with its obligations under the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001* as detailed in each of the Information Privacy Principles (IPP’s) (Refer to Page 9) and the Health Privacy Principles (HPP’s) (Refer to Page 10).

This policy will discuss each of the privacy principles in more detail.

# Scope

This policy applies to all Councillors, Council employees and contractors of the Hobsons Bay City Council. This policy covers all personal and health information collected by Councillors, Council employees and contractors in person, over the telephone, as correspondence or on forms (both paper or electronically) or through Council’s social media and web sites.

# Definitions

1. **Personal information** is information or an opinion, whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
2. **Sensitive Information** is personal information or an opinion about an individual’s racial or ethnic origin, political opinions, trade union membership, philosophical or religious beliefs, sexual preferences or criminal record.
3. **Health Information** is information or an opinion about the physical, mental or psychological health, or disability of an individual or a health service provided or to be provided to an individual.
4. **Information Privacy Principles** (IPP’s) are the ten principles established by the *Privacy and Data Protection Act 2014* that regulate how the Council will collect, hold, manage, use, disclose or transfer personal information.
5. **Health Privacy Principles** (HPP’s)are the eleven principles established by the *Health Records Act 2001* that regulate how the Council as a health service provider will collect, hold, manage, use, disclose or transfer health information.
6. **Public Registers** are documents that Council is required to make publicly available in accordance with State Government legislation. Public Registers may contain personal information and are open to inspection by members of the public. Examples of public registers maintained by Council include a register of building permits pursuant to Section 31 of the *Building Act 1993* and a register of occupancy permits and temporary approvals received by Council pursuant to Section 74 of the *Building Act 1993*.
7. **Privacy Collection Statement** is a statement that appears on every Council developed form or register (both hardcopy and online) that details why the information is being collected by Council, to whom the information will/may be disclosed and why. It specifies any law that requires Council to collect the information and details how an individual can go about gaining access to the information they supply to amend it if required.

# Information Privacy Principles and Health Privacy Principles

The *Privacy and Data Protection Act 2014* contains ten Information Privacy Principles (IPP’s) and the *Health Records Act 2001* contains eleven Health Privacy Principles (HPP’s). These principles regulate how Council will collect, handle, use and disclosure the personal, sensitive and health information it collects.

## Privacy Principle 1 - Collection of personal or health Information

Council will only collect the personal or health information that is necessary in order for it to provide a service and/or carry out its functions and activities. In some instances, Council is required by law to collect this information.

Council will advise individuals, where possible, of the purpose for collecting the information and how they can access this information should they want to correct it. This is done by a Council Officer when dealing in person or over the phone with an individual or by a Privacy Collection Statement when collecting personal information on a Council form or attendance register (both hardcopy and online).

If it is reasonable and practicable to do so Council will only collect personal information directly from that individual. If information is collected about an individual from someone else, Council will take reasonable steps to make sure the individual is made aware of the information that has been collected about them.

Sensitive information will only be collected where the individual has consented, or collection is required or permitted by law. Sensitive information will be treated securely and confidentially and only be used for the purpose for which it was collected.

## Privacy Principle 2 - Use and disclosure of information

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

1. The secondary purpose is directly related to the primary purpose and the individual would reasonably expect Council to use and disclose their information
2. Council has consent of the individual to do so
3. Council is permitted or required by law or it is in the interests of public safety to do so
4. The individual is incapable of giving consent (as defined in the Health Records Act 2001).

## Privacy Principle 3 - Data quality

Council will take reasonable steps to ensure that all personal and health information collected, used or disclosed is accurate, complete and up to date.

## Privacy Principle 4 – Data security and retention

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

Personal and health information will be managed confidentially and securely and destroyed in accordance with relevant legislation specifically the *Public Records Act 1973* and the appropriate General Retention and Disposal Authority.

## Privacy Principle 5 - Openness

Council will make a copy of this Privacy Policy available for download from its website or a copy can be provided on request from Council’s Civic Centre.

On request by an individual, Council will take reasonable steps to let the individual know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds uses and discloses that information.

## Privacy Principle 6 - Access and correction

Individuals have a right to request access to any personal or health information held about them by Council. If an individual believes that their information is inaccurate, incomplete or out of date, they may request Council to correct it.

Council can deny access to personal and health information in accordance with the exemptions detailed in the Privacy and Data Protection Act 2014 and the Health Records Act 2001.

Examples of why Council might deny access to the information include:

1. The matter relates to legal proceedings and the *Freedom of Information Act 1982* applies
2. The release would pose a serious threat to life or health of any person
3. The information is classified confidential.

Where Council denies an individual access to their information it will advise the individual of the reasons for the denial as soon as practicable.

## Privacy Principle 7 – Unique Identifiers

Council will not assign, adopt, use or disclose or require unique identifiers from individuals unless it is necessary to enable Council to carry out any of its functions.

Council will only use or disclose unique identifiers assigned to an individual by another organisation (such as a driver’s licence number, a passport number or a Medicare card number) if it is required in order for Council to carry out its functions or where it has obtained the consent of the individual to use and disclose this information.

## Privacy Principle 8 - Anonymity

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 any limitations to services if the information requested is not provided. For example, Council cannot send an eNewsletter if an individual does not provide their email address in the online registration form.

## Privacy Principle 9 – Trans-border data flows

Council will only transfer personal or health information outside of Victoria in accordance with the provisions outlined in the Privacy and Data Protection Act 2014 and the Health Records Act 2001. For example Council may use cloud computing services based outside Victoria, however it will need to take reasonable steps to ensure that the information which it transfer will not be held, used or disclosed by the host of the information inconsistently with the Victorian Information Privacy Principles and Health Privacy Principles.

## Privacy Principle 10 – Sensitive Information

Council will not collect sensitive information about an individual unless:

1. The individual has provided this information knowingly and with their consent
2. The information is necessary for Council to carry out its functions and/or activities
3. The information is required for research or statistical purposes relevant to government funded targeted welfare or educational services.
4. The disclosure is authorised by law.

## Health Privacy Principles 10 and 11 – Health service provider changes

Council’s Health Services will provide health information to other health providers in accordance with the *Health Records Act 2001*.

Health information relating to a discontinued Council Health Service will be managed in accordance with the *Health Records Act 2001*.

# External contractors

Council may disclose personal information it has collected about an individual where it is necessary for a third party, such as a contractor to carry out a specific job or task. For example personal information is passed onto a contractor by Council for the purposes of a hard waste kerbside collection.

Similarly, contractors may collect, use or disclose personal information about an individual during the course of their duties such as in the case of a contracted Maternal and Child Health nurse. Council requires all contractors to comply fully with the requirements of both the Privacy and Data Protection Act 2014 and the Health Records Act 2001.

# What to do if you believe your personal information has been mishandled

If an individual feels aggrieved by Council’s collection or handling of their personal information, he or she can make a complaint to Council’s Privacy Officer by calling 9932 1047 or by sending written correspondence attention to the Privacy Officer at Hobsons Bay City Council, PO Box 21, Altona, 3018. The complaint will be investigated within five business days and a written response will be provided.

Alternatively, a complaint can be made to the Commissioner for Privacy and Data Protection or the Health Services Commissioner however the Commissioner may decline to hear the complaint if the individual has not made a complaint to Council first.

# Staff training and awareness

All Council employees, including contractors, are required to attend a privacy awareness training session as part of their induction into the organisation. Existing staff members are required to attend a refresher session every three years.

The Employee Code of Conduct specifically addresses the issue of *Privacy and Protection of Information* (page 24) as well as *Confidentiality* of information (Page 14). All staff are given a copy of the Code when they commence with the Council as part of their induction package.

A copy of the Council’s Privacy Policy is available on both the intranet and Council’s website.

# Related documents

1. Privacy and Data Protection Act 2014
2. Health Records Act 2001
3. Local Government Act 1989
4. Freedom of Information Act 1982
5. Public Records Act 1973
6. Employee Code of Conduct (October 2014)
7. 2015-2016 Records Management Policy

# Changes and review

Council may amend this Privacy Policy from time to time to reflect changes in the legislation.

Council will review this Policy two years after its adoption date by CMT.

# Further Information

If an individual has any queries about this Privacy Policy contact should be made with the Council’s Privacy Officer on telephone 9932 1047.

**Appendix A**

**INFORMATION PRIVACY PRINCIPLES (IPP’s)**

*Privacy and Data Protection Act 2014* (Vic)

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Subject |  | Key Principles |
| 1. | Collection | 1.1  1.3 | An organisation (including a person) must not collect personal information about an individual unless the information is necessary for one or more of its functions or activities  At or near the time of collection, the organisation must notify the individual of a range of prescribed matters including the identity of the organisation, the purpose, proposed use and disclosure, right to access etc |
| 2. | Use and disclosure | 2.1 | An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless a prescribed exception applies |
| 3. | Data quality | 3.1 | An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date |
| 4. | Data security | 4.1 | An organisation must take reasonable steps to protect personal information it holds from misuse and loss and from unauthorised access, modification or disclosure  An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose |
| 5. | Openness | 5.1  5.2 | An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it  On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information |
| 6. | Access and correction | 6.1  6.5 | If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that prescribed exceptions apply  If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete or up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date |
| 7. | Unique identifiers | 7.1  7.2 | An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently  An organisation must not adopt as its own identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless prescribed exceptions apply |
| 8. | Anonymity | 8.1 | Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation |
| 9. | Transborder data flows | 9.1 | An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if prescribed conditions apply |
| 10. | Sensitive information | 10.1 | An organisation must not collect sensitive information about an individual unless the individual has consented or prescribed exceptions apply |

**HEALTH PRIVACY PRINCIPLES (HPP’s)***Health Records Act 2001* (Vic)

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Subject |  | Key Principles |
| 1. | Collection | 1.1  1.4 | An organisation (including a person) must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and the individual has consented.  At or near the time of collection, the organisation must notify the individual of a range of prescribed matters including the purpose, proposed use and disclosure, right to access etc. |
| 2. | Use and disclosure | 2.1  2.2 | An organisation may use health or personal information about an individual only for the primary purpose for which the information was collected.  An organisation must not use or disclose health information about an individual for a purpose other than the primary purpose unless the individual has consented to the use or disclosure |
| 3. | Data quality | 3.1 | An organisation must take reasonable steps to make sure that the health information it collects, uses or discloses is accurate, complete and up to date and relevant to its functions |
| 4. | Data security and retention | 4.1  4.2 | An organisation must take reasonable steps to protect the health information it holds from misuse and loss and from unauthorised access, modification or disclosure  A health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate unless prescribed conditions apply |
| 5. | Openness | 5.1  5.2 | An organisation must set out in a document its health information management policies, and access rights, and must make the document available to anyone who asks for it  On request by an individual, an organisation must take reasonable steps to advise the individual about whether it holds their health information, how and why it is held, and the process for seeking access |
| 6. | Access and correction | 6.1  6.5 | If an organisation holds health information about an individual, it must provide the individual with access to the information on request by the individual, unless prescribed conditions apply  If an individual is able to establish that their information held by an organisation is inaccurate, incomplete, misleading or out of date, the organisation must take reasonable steps to correct the information |
| 7. | Identifiers | 7.1  7.2 | An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently  A private sector organisation may not adopt as its own identifier of an individual an identifier that has been assigned to that person by a public sector organisation unless prescribed exceptions apply |
| 8. | Anonymity | 8.1 | Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation |
| 9. | Transborder data flows | 9.1 | An organisation may transfer health information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if prescribed conditions apply |
| 10. | Transfer or closure of the practice of a health service provider | 10.1 | If the practice or business of a health service provider is to be transferred or closed, the provider must comply with a prescribed set of procedures, including notification to former clients and the public |
| 11. | Making information available to another provider | 11.1 | If an individual requests a health service provider to make their health information available to another provider, the former must comply with the request |

# Document Control

|  |  |
| --- | --- |
| **Policy:** | Privacy Policy (A232093) |
| **Date prepared:** | 12th February 2016 |
| **Dated adopted by CMT:** | 17th March 2016 |
| **Directorate:** | Corporate Services |
| **Department:** | Information Services |
| **Responsible Officer(s):** | Manager Information Services  CEO and Directors  Departmental Managers  Coordinators, Team Leaders and Supervisors  System Administrators  All Staff  Councillors, Contractors and Volunteers |
| **Next Review Due:** | 17th March 2018 |
| **Applicable Legislation**  A range of legislation, statutes and codes of practice are applicable to information security within the Council. This may include, but is not limited to: | *Privacy and Data Protection Act 2014*  *Health Records Act 2001*  *Local Government Act 1989*  *Freedom of Information Act 1982*  *Public Records Act 1973* |
| **Related Policies:** | Employee Code of Conduct ([Pulse Link](http://hbintranet.hobsonsbay.vic.gov.au/files/f7cac6bf-730b-48a6-b7b4-a3f700b28cd4/Hobsons_Bay_Code_of_Conduct_-_Oct_2014.pdf))  Records Management Policy (A2066460) |
| **Related Procedures:** | ICT Standards and Procedures. |

**Approvals**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version Number** | **Date** | **Created/ Reviewed by** | **Issued To** | **Purpose/Outcome** |
| 1.0 | 29-10-2009 | Chris Eddy  (Policy inception) | IT CDST and Consultative Committee | Endorsed |
| 1.2 | 23-02-2016 | Julie Brne  Roger Verwey | IT Steering Committee | Feedback received and included in revised policy |
| 1.2 | 17-03-2016 | Julie Brne  Roger Verwey | CMT | Endorsed |

*- End of Document -*