Information Privacy Policy

POLICY STATEMENT

The City of Port Phillip believes that the responsible handling of personal information is essential to good corporate governance and is strongly committed to protecting an individual's right to privacy. Accordingly, Council is committed to full compliance with its obligations under the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001*.

In particular, Council complies with the Information Privacy Principles (IPPs) and Health Privacy Principles (HPPs) contained in the *Privacy and Data Protection Act 2014* and the *Health Records Act 2001*. Obligations under these Acts apply to Councillors, Council staff (employees), agents (consultants, agency staff and volunteers) and contracted service providers.

This document outlines the Information Privacy Principles and details guidelines and processes as to how Privacy and Data Protection Policy should be implemented in practice in the Council and how they will apply to the community.

For further information regarding Council's obligations to comply with the Health Privacy Principles please refer to Council's Health Records Policy:
http://www.portphillip.vic.gov.au/default/CommunityGovernanceDocuments/Council_Health_Records_Policy.pdf

A basic overview of the key differences between the HPPs and IPPs can be found:
https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-information-sheets

PURPOSE

The main purposes of the *Privacy and Data Protection Act 2014* are:

- to provide for responsible collection and handling of personal information in the Victorian public sector; and
- to provide remedies for interferences with the information privacy of an individual; and
- to establish a protective data security regime for the Victorian public sector; and
- to establish a regime for monitoring and assuring public sector data security; and
- to establish the Commissioner for Privacy and Data Protection; and
- to repeal the Information Privacy Act 2000 and the Commissioner for Law Enforcement Data Security Act 2005 and make consequential amendments to other Acts.

SCOPE

This policy is applicable to Councillors, Council staff, agents, contracted service providers, residents, ratepayers and other members of the community, whose personal information and health records are collected by Council.

Any reference to Council or Council staff in this policy includes Councillors, agents (consultants, agency staff and volunteers) and contracted service providers.

In some instances, personal and health information may be collected, used and disclosed on Councils behalf by agents and contracted service providers.

DEFINITIONS

Agent is an individual or organisation employed by Council to perform a service that involves handling personal information. An agency relationship will mean that Council will usually be held responsible for how their agents (like their employees) handle personal information.

Contracted Service Provider (CSP) is a service provider which is required to comply with the Privacy and Data Protection Act 2014 and the Information Privacy Principles due to entering into a contract.

A document may be in writing, electronic or paper format and may refer to books, scans, photographs, emails and documents stored in a physical file, database or spread sheet.

Health information means (in relation to an individual) information or an opinion about the physical, mental or psychological health, a disability, the individual's express wishes about the future provision of health services to him/her or a health service provided or to be provided, personal information collected to provide a health service or the dispensing on prescription of a drug or medicinal preparation by a pharmacist. Council may request health information in order to provide services to the community, for example; aged care service.

HPPs – Health Privacy Principles is a set of principles under the Health Records Act 2001 that regulates the handling of health information.

IPPs – Information Privacy Principles is a set of principles under the Privacy and Data Protection Act 2014 *that regulates the handling of personal information.*

Personal information means information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion, other than certain health and generally available information (to which the Health Records Act 2001 applies). Examples of personal information collected or handled by Council might include names, addresses, telephone numbers, date of birth, Medicare number, or the motor vehicle registration of an individual. This information is collected for specific purposes, for example; to provide planning, valuation and property services and parking permits. Council may also request personal information in order to provide education, welfare and other community services (childcare services, holiday programs). In some instances, personal information may be contained on a public register, for example; register of building permits, food premises and animal registration details.

Privacy Impact Assessment (PIA) is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated".

Public registers hold documents that are open to inspection by members of the public and contain information required or permitted by legislation.

Sensitive information includes information or an opinion about an individual's racial or ethnic origin, political opinions, trade union membership, philosophical or religious beliefs, sexual orientation or criminal record.

Social media is an umbrella term that defines the various activities that integrate technology, social interaction and the construction of words, pictures, video, and audio. For example; blogs, instant messaging, podcasts, forums and postings.

Third party, in relation to personal information means a person or body other than the organisation holding the information and the individual to whom the information relates.

OBJECTIVE

The objective of this policy is to ensure the responsible collection and handling of personal and health information relating to individuals by compliance with the Information Privacy Principles (IPPs).

ADMINISTRATION

Council's Governance Advisor is the Council's Information Privacy Officer. The Information Privacy Officer has the responsibility to assist Council comply with its obligations under the Privacy and Data Protection Act 2014 and is authorised to provide advice and receive complaints and requests for access and correction. The Information Privacy Officer may be required to seek legal advice if required.

The Information Privacy Officer is responsible for preparing and periodically updating the policy and guidelines and submitting them to the Executive Management Team for approval, ensuring that staff understand the Privacy Policy and, when necessary, liaising with the senior management group to ensure compliance with the Act. The Information Privacy Officer is responsible for organising regular privacy training across the organisation for all Council staff.

The Information Privacy Policy will be reviewed from time to time to take into account significant changes in legislation that are made that affect the accuracy of the policy document or as required by the Executive Management Team.

POLICY GUIDELINES AND PROCEDURES

Council must comply with the ten Information Privacy Principles contained in the Act, listed below:

IPP1 Collection
IPP2 Use and Disclosure
IPP3 Data Quality
IPP4 Data Security
IPP5 Openness
IPP6 Access and Correction
IPP7 Unique Identifiers
IPP8 Anonymity
IPP9 Transborder Data Flows
IPP10 Sensitive Information

A detailed explanation of each of the IPPs is available from the Privacy Victoria website at the following link:
https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-guidelines

Council will manage personal information as outlined in the following principles:

Principle 1 – Collection

Council will only collect personal information that is necessary for specific and legitimate functions of Council. Information will be collected by fair and lawful means and not in an unreasonably intrusive manner.

Guidelines (for Principle 1)

Council will advise individuals, where possible, of the purposes for which their personal information is being collected, and of those third parties to whom the information may be disclosed.

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

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

As required by legislation, Council invites submissions from the general public and collects contact details for the purpose of responding to submissions in accordance with legislation.
Contact details are also collected from individuals interested in being informed about and participating in Council programs and events. Contact details are also collected from individuals who wish to receive publications on programs and events.

Personal information is also collected through social media. Employees who use social media at the Council are required to adhere to this policy and the Social Media Policy
http://intranet.portphillip.vic.gov.au/secured/social-media.htm

Our website can be visited anonymously because the site does not collect or record personal information other than the information an individual chooses to provide by email or internet forms.

When collecting personal or health information, Council will take reasonable steps to advise what information is being sought, for what purpose, whether any law requires the collection of the information and the main consequences, if any, of not providing the information.

Forms collecting information that is being used for a specific purpose must include a privacy statement on the form including the purpose of the collection.

The Information Privacy Officer will:

- conduct an ongoing review of all forms within the organisation that collect personal and health information and ensure that an appropriate privacy statement is included;
- establish and maintain a 'Register of Forms' with privacy statements; and
- regularly email staff reminding them of their obligations under the Privacy and Data Protection Act 2014 and request that Governance be advised of any new forms which may require or have a privacy statement so that the 'Register of Forms' can be updated.

Council's privacy statements will be published in the relevant publications, for example; forms, website, advertising material and correspondence requesting personal or health information.

> A privacy statement template may be modelled on the following:
> "The personal information requested on this form is being collected by the council for [*insert purpose and any law that requires the particular information to be collected*]. The personal information will be used solely by the council for that primary purpose or directly related purposes. Council may disclose this information to [*list organisations and why*]. If this information is not collected [*insert consequences, if any*]. The applicant understands that the personal information provided is for the [*insert functional purpose*] and that he or she may apply to the council for access to and/or amendment of the information. Requests for access and or correction should be made to Council's Privacy Officer".

Council staff should have a clear purpose for collecting each piece of personal information. They should work this purpose out before collecting the information. Collecting information with no identifiable purpose is not acceptable.

Currently, Council provides a wide range of services to the community within a broad legislative environment. Council holds personal information for the purposes of enabling subsequent contact, ascertaining correct property ownership within Council's boundaries and allocating rate liability further, undertaking specific client functions within various service environments.

Sometimes, Council staff receive personal information that is not necessary for or related to any purpose of Council. This includes:

- when people send information to Council without Council asking for it; or
- when Council asks for some information, but individuals provide more information than asked for.

As soon as practical after it receives personal information, Council should decide whether it is relevant to what Council does. If information is not relevant, Council should not keep it in its records. Council should also give consideration to the *Public Records Act 1973* which takes precedence over the *Privacy and Data Protection Act 2014* when performing this activity, for example; Is this a defined public record?

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:

- It is for a related purpose that the individual would reasonably expect;
- Council has the consent of the individual to do so;
- If, as defined by the *Health Records Act 2001*, the individual is incapable of giving consent;
- As required or permitted by the Privacy and Data Protection Act 2014 or any other legislation.

Council may be required to disclose personal information to law enforcement agencies or under direction of a court. Any other bodies requesting personal information would be required to specify the relevant legislation that entitles them to the release of the information.

Guidelines (for Principle 2)

In certain circumstances and in accordance with law, documents related to Council functions may be referred to relevant government departments or contracted service providers.
Some de-identified personal information from enquiries and complaints is used in submissions, applications and reports to Council, but never in a way that would compromise an individual's privacy. De-identified information may be shared with other privacy regulators and for awareness and reporting functions.
Council staff are required to handle all personal and health information with discretion and to comply with the Privacy and Data Protection Act 2014.

Use is interpreted broadly. It relates to managing personal information within the course of Council business. This includes:

- searching records for any reason;
- using personal information in a record to make a decision;
- inserting personal information into a database.

Disclosure may be interpreted as, a release, publication or revelation of personal information by the Council. A disclosure can occur both within Council and to outsiders of the Council.

For example:

- providing personal information to a third party whom the Council has contracted to work for it;
- providing a record containing personal information to a member of the public;
- leaving personal information on a whiteboard in the Council that other officers may see;
- setting up a computer logon which allows someone outside Council to access personal information, there is a disclosure each time the outside person accesses the information using that means.

Further, disclosure takes place when members of the public access registers that Councils are required by law to make public.

Principle 3 – Data Quality

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

Guidelines (for Principle 3)

Council is responsible for the quality of the personal information it holds. Council is required to take all reasonable steps to ensure that the personal information it holds is accurate and, given the purpose of the information, is relevant, up to date, complete and not misleading. It is therefore the responsibility of Council to ensure that the personal information it holds is of high quality.

These are continuing obligations. Council must take reasonable steps to ensure the quality of the personal information it holds is accurate, complete and up to date throughout the period it holds the information.

Principle 4 - Data Security and Retention

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

Personal and health information will be managed confidentially and stored securely.

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

Council will implement a clean desk policy for nominated high risk areas who manage the majority of Council's personal and health information and who are at greater risk of non-compliance with the Privacy and Data Protection Act 2014.

Council will ensure software and hardware safeguards are in accordance with Council's Information Security Management Framework, together with access controls, secure methods of communication and back-up disaster recovery systems to protect personal and health information.

Council's Digital and Technology Services department have developed an Information and Communication Technology (ICT) user policy http://intranet.portphillip.vic.gov.au/secured/ict-policy.htm

All council employees, councillors, contractors, vendors and third parties who use the organisation's ICT resources directly and remotely are required to ensure their use of Council's information and Communication Technology (ICT) systems, applications and information is effective, responsible, safe, ethical and lawful.

Personal and health information will be de-identified, archived or destroyed in accordance with the *Public Records Act 1973* and the General Retention and Disposal Authority for Records of Common Administrative Functions Version 2009 (PROS 07/01).

Guidelines (for Principle 4)

Council policy relates to the security of personal and health information, both electronic and paper-based, which is accessible to staff, explaining what security measures need to be taken, what needs to be done, when and by whom and gives practical advice on situations that regularly arise in particular areas of the organisation.

The Information Privacy Officer will be available to discuss cases where the appropriate security measures are not clear. Council will take into consideration their obligations under the *Public Records Act 1973*, bearing in mind that it will take precedence over the Privacy and Data Protection Act 2014.

The Information Privacy Officer will identify departments and / or staff within Council that are exposed to greater risk of non-compliance with the Privacy and Data Protection Act 2014. A clean desk policy, under which all papers are required to be securely stored at the end of the working day will apply to those individuals and departments that are identified as 'high risk' and a review of storage facilities will be undertaken and secure storage provided where required.

Filing cabinets, safes, compactuses containing records of personal information should not be left unlocked. All paper records containing personal information should be stored securely and/or recorded on appropriate databases. Files should have security classifications reflecting the importance or sensitivity of the records held on them. Storage and access arrangements should reflect the security classification.

Movements of files should be recorded on Council records management system, particularly if the files are being forwarded to another office.

Whilst a clean desk policy will only be implemented for 'high risk' departments and / or staff, securely storing papers at the end of the working day rather than leaving them on the desk, is good practice across the organisation. This reduces the risk of personal information being seen or taken by unauthorised people.

Principle 5 - Openness

Council's Information Privacy Policy will be available on the Port Phillip website, Councils Intranet and by request.

Guidelines (for Principle 5)

Information Privacy Principle 5 reflects the fact that, in order to be able to exercise their other rights in relation to the personal information that Council holds about them, people must be able easily to find out:

- the existence of personal information systems that affect them;
- the nature and extent of those systems;
- the main purposes and uses of those systems; and
- how to gain access to personal information held in them.

Principle 6 - Access and Correction to Information

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

Council must take reasonable steps to correct information so that it is accurate, complete and up to date. Where the Council holds personal information about an individual and the individual is able to establish that the information is incorrect, Council will undertake to correct that information within 14 days. If the request is submitted under the Freedom of Information Act 1982, it will be processed as soon as practicable or within 45 days. Should access or correction be denied, reasons will be provided.

The process for requesting access to documents containing personal and health information held by the Council will be handled in accordance with the Freedom of Information Act 1982 and should be addressed to the Freedom of Information Officer, City of Port Phillip, Private Bag No.3, Post Office St Kilda, Victoria, 3182.

Guidelines (for Principle 6)

If Council possesses or controls a record that contains personal information, it shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

- is accurate; and
- is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

Access to personal information held by Council must be requested in writing from Council's Information Privacy Officer, and must be adequate to identify the identity of the applicant.

Principle 7 - Unique Identifiers

Council will not assign, adopt, use, disclose or require unique health or other identifiers for individuals except for the course of conducting normal business or if allowed or required by law. Examples of unique identifiers belonging to other organisations include tax file numbers, social security identification numbers, drivers licence numbers.

Guidelines (for Principle 7)

A unique identifier is a string of characters, usually a number, used to identify particular individuals. Council can use unique identifiers to manage their affairs and identify their clients; this is often an essential tool for ensuring high data quality and providing a high standard of service. Council shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable Council to carry out any one or more of its functions effectively and it has obtained the consent of the individual.

Council shall not assign to an individual a unique identifier that, to Council's knowledge, has been assigned to that individual by another agency.

If Council assigns unique identifiers to individuals all reasonable steps should be taken to ensure that unique identifiers are assigned only to individuals whose identity is clearly established;

Council shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which the unique identifier was assigned or for a purpose that is directly related to one of those purposes.

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, particularly if they are seeking general information.

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

Guidelines (for Principle 8)

Related to limitations on the collection of personal information is the idea that where possible, people should be able to go about their business anonymously. People should have the option of not identifying themselves when entering transactions.

This principle is applicable to the design of information systems (although it is equally applicable whenever a person is required to give their name and address); once a system is in place, its informational requirements are often inflexible. The popularity of anonymising features on the internet suggests both that many people see maintaining anonymity as an important part of defending their information privacy, and that in the electronic environment it is often feasible to restrict the collection of identified information while still providing people and organisations the confidence they need to transact their business.

While the option of anonymity gives people an opportunity to protect their privacy, a qualification like ‘where possible’ or ‘where practicable' is necessary to accommodate situations where the effectiveness of a system requires the collection of personal information.

Principle 9 - Transborder Data Flows (Transfer of Information Outside Victoria)

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*.

Guidelines (for Principle 9)

Council may transfer personal information about an individual outside Victoria only if:

- Council reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles; or
- the individual consents to the transfer; or
- the transfer is necessary for the performance of a contract between the individual and Council, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between Council and a third party; or all of the following apply:
    - the transfer is for the benefit of the individual;
    - it is impracticable to obtain the consent of the individual to that transfer;
    - if it were practicable to obtain such consent, the individual would be likely to give it; and
    - Council has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

Principle 10 - Sensitive Information

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 2014.

Sensitive information is also evident and collected through social media. Council employees who use social media are required to adhere to the Social Media Policy which is accessible on Council's intranet.

Guidelines (for Principle 10)

"Sensitive information" means information or an opinion about an individual's:

- race or ethnic origin; or
- political opinions; or
- membership of a political association; or
- religious beliefs or affiliations; or
- philosophical beliefs; or
- membership of a professional or trade association; or
- membership of a trade union; or
- sexual orientation; or
- criminal record – that is also personal information (see Schedule 1 of the Privacy and Data Protection Act 2014)

Some examples of sensitive information that may be required to be collected by Council are:

- provision of meals that are appropriate to a person's faith;
- medical restrictions that are appropriate to a person's faith, for example; blood transfusions
- union membership details
- criminal records

Council must ensure that any sensitive information collected must be stored confidentially and securely in accordance with Information Privacy Principle 4 – Data Security and Retention.

Council must not collect sensitive information about an individual unless:

- the individual has consented; or
- the collection is required by law; or
- the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
    - is physically or legally incapable of giving consent to the collection; or
    - physically cannot communicate consent to the collection; or
- the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

However, Council may collect sensitive information about an individual if the collection:

- is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
- is information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and
- there is no reasonably practicable alternative to collecting the information for that purpose; and
- it is impracticable for the organisation to seek the individual's consent to the collection.

RESPONDING TO A PRIVACY COMPLAINT

The complaint process is available to any person who feels aggrieved by Council's handling of their personal information, or believes that an officer of the Council is in breach of the Privacy and Data Protection Act 2014 or *Health Records Act 2001*.

A complaint should be directed to Council's Privacy Officer. Contact details are as follows:
Privacy Officer
City of Port Phillip
Private Bag No.3
P.O. Box St Kilda Vic 3182

Telephone: 9209 6692

Email: governance@portphillip.vic.gov.au

Definition of a formal complaint

- The complaint must be in writing (email is acceptable); and accompanied by a suitable form of identification, such as a photocopy of a driver's licence;

- The complaint must provide a brief description of the incident, for example; date of the incident, what personal information was involved (name, address, government issued identification, financial, medical) and what form was it in, for example; paper records, electronic database;

- The complainant must be the person who is directly involved in the complaint or the person making the complaint must be authorised in writing to represent the person directly involved in the complaint. The person directly involved in the complaint must be competent to make a complaint and must be over the age of 18 or of sufficient maturity to fully understand the nature and significance of the complaint being made;

- The complainant may withdraw a complaint at any time. A request for a withdrawal of a complaint must be sent in writing to the Information Privacy Officer.

Process

When a complaint is received that is deemed to be a formal complaint, the Council's Information Privacy Officer will be assigned to handle the complaint as the investigating officer. The complaint will be assessed and processed in accordance with the City of Port Phillip "Privacy Complaint Response Procedure".

Alternatively, a complaint may be made to the Commissioner for Privacy and Data Protection (although the Commissioner may decline to hear the complaint if a complaint has not first been made to Council).

Where the complainant is not satisfied with the decision of the Information Privacy Officer s/he may apply to the Commissioner for Privacy and Data Protection or the Victorian Health Services Commissioner for further action.

RESPONDING TO A PRIVACY BREACH

A privacy breach occurs when personal, sensitive or health information of an individual is misused, lost or subjected to unauthorised access, modification or disclosure by Council.

The City of Port Phillip Privacy Breach Procedure sets out the process to be followed by all Council staff in the event that the Council experiences a privacy breach, suspects that a privacy breach has occurred or has received a complaint.

This procedure involves a four step process in responding to a privacy breach:

Step 1	Contain the breach and make a preliminary assessment;
Step 2	Evaluate the risks for individuals associated with the breach;
Step 3	Consider breach notification to affected individuals and others (not all breaches warrant notification). Is there a risk of serious harm? Risk assessment to be undertaken on a case by case basis;
Step 4	Review the incident and take action to prevent future breaches; fully investigate the cause of the breach and implement prevention strategies and prevention action plan.

Preventative actions will be monitored by the responsible Manager and the Privacy Officer and actions reported to the Privacy Officer when completed. Outstanding actions will be reported to the Executive Leadership Team.

All privacy breaches are reported to the Executive Leadership Team, reported to Council via the CEO's monthly report and to the next applicable Audit and Risk Committee meeting. Privacy breaches will be recorded in the "Non-Compliance Issues Register" maintained by Governance.

SENDING EXTERNAL GROUP EMAILS

To mitigate any risk of an external email privacy breach, a procedure for sending external group emails has been developed for all staff to adhere to prior to sending an external email to more than one external email recipient (group). A copy of this procedure is handed out to all staff by Governance as part of the employee's induction program http://intranet.portphillip.vic.gov.au/secured/administration_information_protocols.htm.

OR

For Council staff that regularly send group emails, Council's Digital and Technology Services department have implemented an online tool that can be used to create address lists, send and track emails safely and securely. This tool can be used to further mitigate the risk of a group external email privacy breach.

INFORMATION PRIVACY TRAINING

Information privacy training and refresher training after a period of one year, is mandatory for all employees or other persons otherwise engaged by Council with a City of Port Phillip email address. In addition, during the year tailored privacy training sessions will be facilitated by Council's Information Privacy Officer. The Executive Leadership Team will receive monthly status reports on the percentage of mandatory information privacy training undertaken across the organisation.

PRIVACY IMPACT ASSSESSMENT

In designing or managing any project or system, there may be several competing public interests to be considered, including the protection of privacy and privacy risk. A privacy "risk" means the risk that a project will not comply with privacy laws, will not meet community expectations, or will have unmitigated or unnecessary negative impacts.

It is strongly encouraged that staff complete a Privacy Impact Assessment (PIA) to consider the future consequences of a current or proposed action and look to prevent or minimise any negative impacts on privacy. The Privacy Impact Assessment template is available from the Office of the Victorian Information Commissioner's website.

Assessments are to be conducted in accordance with the "How to conduct a Privacy Impact Assessment" process.

BREACHES OF THE PRIVACY AND DATA PROTECTION ACT 2014

The Council may incur penalty units for breaches under the Privacy and Data Protection Act 2014. Disciplinary actions outlined in the Councillor Code of Conduct, Employee Code of Conduct and the Code of Conduct for consultants, agency staff and volunteers may also apply to individuals who have breached the privacy of another individual.

OTHER LEGISLATION

Other Acts that relate to the *Privacy and Data Protection Act 2014* are the *Freedom of Information Act 1982* and the *Health Records Act 2001*.

If the Privacy and Data Protection Act 2014 is inconsistent with a provision made under other legislation (such as the *Freedom of Information Act 1982*), that other provision prevails.

RELATED DOCUMENTS

- *City of Port Phillip Code of Conduct for Consultants, Agency Staff and Volunteers*
- *City of Port Phillip Employee Code of Conduct*
- *City of Port Phillip Health Records Policy*
- *City of Port Phillip Social Media Policy*
- *Councillor Code of Conduct*
- *Freedom of Information Act 1982*
- *Health Records Act 2001;*
- *Privacy and Data Protection Act 2014;*
- *Local Government Act 1989*
- *Protected Disclosure Act 2012*
- *Public Records Act 1973*

ENDORSEMENT

This policy was endorsed by the Executive Management Team on 7 May 2018 and will be reviewed at least every three years.

In June 2019, as required by the Executive Management Team, this policy in the section "Information Privacy Training" was further reviewed and updated by the Director Chief Executive Officer's Office.