Privacy Policy

CD16435[v2]

Banyule
City Council

Document Control

Record Number	CD16435[v2]
Date Created	25 November 2015
Next review date	1 August 2026
Business Unit	Governance & Integrity
Responsible Officer	Manager Governance and Integrity
Date of Approval	7 August 2024

Updates to this Policy

From time-to-time circumstances may change requiring minor administrative changes to this policy. Updates will be made where they do not have a material impact on the document such as changes to names, document references and/or minor updates to legislation. Any change or update which materially alters the document must have Executive Management Team endorsement.

Acknowledgement of the Traditional Custodians

Banyule City Council proudly acknowledges the Wurundjeri Woi-wurrung people as Traditional Custodians of the land and we pay respect to all Aboriginal and Torres Strait Islander Elders, past, present and emerging, who have resided in the area and have been an integral part of the region's history. We recognise and value the ongoing contribution of Aboriginal people and communities to Banyule life and how this enriches us. We embrace the spirit of reconciliation, working towards the equality of outcomes and ensuring an equal voice.

Diversity Statement

Our community is made up of diverse cultures, beliefs, abilities, bodies, sexualities, ages and genders. We are committed to access, equity, participation and rights for everyone: principles which empower, foster harmony and increase the wellbeing of an inclusive community.

Contents

1. About this Policy

Banyule City Council (Council) provides many services to its community. The role of Council is to provide good governance in our City for the benefit and wellbeing of the community giving effect to the overarching governance principles outlined in the *Local Government Act 2020.*

Council has a wide range of obligations under many pieces of Victorian legislation including managing and protecting the personal and health information of individuals that we collect and use. We are also guided by our corporate and public policies and local laws.

The *Privacy and Data Protection Act 2014 (PDP Act)* and the *Health Records Act 2001 (HR Act)* prescribes the Information Privacy Principles (IPPs) and the Health Privacy Principles (HPPs) outlined below that Council are required to comply with to promote and ensure the fair and responsible collection and handling of personal and health information.

Information Privacy Principles (IPPs)

Principle 1	Collection
Principle 2	Use and Disclosure
Principle 3	Data Quality
Principle 4	Data Security
Principle 5	Openness
Principle 6	Access and Correction
Principle 7	Unique Identifiers
Principle 8	Anonymity
Principle 9	Transborder Data Flows
Principle 10	Sensitive Information

Health Privacy Principles (HPPs)

Principle 1	Collection
Principle 2	Use and Disclosure
Principle 3	Data Quality
Principle 4	Data Security
Principle 5	Openness
Principle 6	Access and Correction
Principle 7	Unique Identifiers
Principle 8	Anonymity
Principle 9	Transborder Data Flows
Principle 10	Transfer or closure of the practice of a health service provider
Principle 11	Making information available to another health service provider

Council Plan Reference

The Privacy Policy links to the following Strategic Objective contained within our Council Plan 2021-2025.

> 'A responsive, innovative and engaged Council that has the trust of our community through demonstrated best practice governance, is financially sustainable, and advocates on community priorities and aspirations.'

Relevant Legislation

- *Privacy and Data Protection Act 2014*
- *Health Records Act 2001*
- *Freedom of Information Act 1982*
- *Surveillance Devices Act 1999*
- *Charter of Human Rights and Responsibilities Act 2006*
- *Gender Equity Act 2020*

Relevant Documents

- CD18538 Information Security Policy
- CD18522 Surveillance in Public Places Policy
- CD17736 Public Transparency Policy
- CD18609 Call Recording Operating Policy
- CD15487 Public Interest Disclosure Procedures
- CD17048 Freedom of Information - Part II Statement
- CD14452 Fraud and Corruption Control Framework
- CD14678 Information Management Policy
- F2022/1190 IT Policies and Procedures
- CD15753 Staff Code of Conduct
- CD6176 Councillor Code of Conduct
- CD5196 Disciplinary Policy and Procedures

2. Policy Statement

Banyule City Council believes that the responsible handling of personal and health information is a key aspect of good governance and an integral part of its commitment towards accountability and integrity and is strongly committed to protecting an individual's right to privacy.

Council is committed to managing the personal and health information we hold in accordance with the IPPs in the *PDP Act* and the HPPs in *HR Act.* This Privacy Policy outlines some of these Principles and how they will apply.

3. Scope

This policy applies to all Councillors, Council officers, volunteers and contractors (including subcontractors) of Banyule City Council.

It applies to all personal and health information collected and held by Council, including information received from a third party.

4. Definitions

Personal information	means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Examples of personal information may include: • name; • date of birth • blood type, DNA code, fingerprints; • home/work address, contact number/s and email address; • credit card details; • drivers licence; • photographs and video footage.

Sensitive information	is recorded information or opinion, whether true or not, about a readily identifiable individual (or an individual whose identity can be reasonably ascertained) that includes: • Racial or ethnic origin; • Political opinions or membership of a political association; • Religious beliefs or affiliations; • Philosophical beliefs; • Membership of a professional or trade association, or a trade union; • Sexual preferences or practices; or • Criminal record.
Health Information	is broadly defined to include information or an opinion about the physical, mental or psychological health of an individual, a disability, an individual's expressed wishes for future provision of health services or any health service provided to an individual, or other information collected to provide or in providing a health service.
Primary Purpose	the primary purpose is one for which the individual concerned would expect their information to be used or disclosed. Using the information for this purpose would be within their reasonable expectations.
Secondary Purpose	a secondary purpose is related to the primary purpose of collection and the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose.
Unique Identifier	an identifying name or code (usually a number) assigned by an organisation to an individual to uniquely identify that individual for the purposes of the operations of the organisation. This does not include an identifier that consists only of the individual's name.
Publicly Available Information	are documents that Councils are required to make publicly available pursuant to legislation. These registers: • are open to inspection by members of the public; • contain information required or permitted by legislation; • may contain personal information.

5. Policy Principles

The ten (10) Information Privacy Principles (IPPs) and the eleven (11) Health Privacy Principles (HPPs) are the practical core of the *PDP Act and HR Act*. With limited exemptions, they guide us on how we must manage an individual's personal and health information when they interact with us. Protecting the privacy of individuals by handling their information in accordance with the principles is embedded in Council's practices.

Principle 1 – Collection (IPP1/HPP1)

We will only collect personal and health information that is necessary for our functions and activities. In some instances, Council is required by law to collect this information. What we collect will differ from service to service.

We collect health information where it is necessary to facilitate a health service or program such as maternal and child health service, childcare service, immunisation program, aged care service. Typically, collection may include:

Personal Information	Health Information
• name;	• information about an illness, injury or disability;
• address (home, postal and e-mail);	• notes of symptoms or a diagnosis;
• telephone numbers (work, home, mobile);	• information about a health service had or that will be received.
• date of birth;	
• credit card and bank account numbers.	

We will only collect sensitive or health information where you have consented or as permitted under legislation. This information will be collected by fair and lawful means and not in an unreasonably intrusive way.

If it is reasonable and practical to do so, we will collect personal and health information directly from an individual. We will only collect an individual's information from an authorised representative if the individual's consent is provided or as permitted under legislation.

Collection Notices

We will inform individuals of the matters set out in the Acts via a collection notice that explains why and the purpose in which the information is being collected, how we will use and handle the information, any relevant laws, and consequences for the individual if all or part of the information is not collected.

Collection notices may be provided in a variety of ways, including verbally such as during phone calls, written writing on physical and online forms, on our website, and signage displayed at events where recording is taking place.

Surveillance Activities

We use surveillance systems in public places (e.g. CCTV) where it is lawful to do so, and it is fair and reasonably necessary to perform the functions or activities of Council. Council's Surveillance in Public Places Policy regulates the operation and management of Council owned surveillance systems used on Council property, assets and in public places to ensure that systems are installed in accordance with the Surveillance Devices Act 1999.

Personal and health information collected in surveillance data are subject to the IPPs and HPPs and will be managed in accordance with this policy. Monitoring and access to surveillance data is controlled and managed in accordance with the relevant system operating procedures.

Body Worn Cameras

Body worn cameras are used by officers to assist in the deterrence, prevention and monitoring of incidents involving interactions with members of the public, to improve safety in the workplace and to assist with investigations. Officers may make recordings of members of the public using a body worn camera when:

- exercising an authorised legislated power and the recording would assist in collecting evidence; and
- other occasions when the officer believes a recording is necessary:
    - that an offence is being committed, has been committed or is about to be committed,
    - where there is an occupational health and safety issue;
    - that would provide transparency of a public interaction;
    - in connection with an enforcement or non-compliance activity.

The use of body worn cameras is in accordance with the Surveillance Devices Act 1999. Any personal and health information recorded using body worn cameras are managed in accordance with this policy.

Photographs, Video and Audio Recordings

We may take photographs, video or audio recordings on Council premises, from assets (eg. Waste trucks), in public places and when someone calls us.

Inbound calls are recorded and used as a tool to coach and train staff and improve customer service outcomes in accordance with our Call Recording Operating Policy. Recordings may also be used to investigate and respond to complaints and incidents in accordance with our Customer Complaint Management Policy and the Unreasonable Customer Behaviour Policy.

Council meetings are recorded and live streamed as outlined in our Public Transparency Policy which aims to improve meeting accessibility, increase community awareness, and to build transparency and confidence in the integrity and accountability of the decision-making process. Recordings of the live stream are made publicly available on our website and Facebook page after the meeting. Public speakers addressing the Council are visible on the livestream and included on the recording. Any comments made by members of the gallery, may also be captured on the live stream,-and recorded and publicly available on the meeting footage.

Images and recordings may also be taken for publicity purposes. Consent will be sought from individuals prior to capture (if practicable). Where it is not practical to obtain consent during public events or in public places, we may use other methods to inform individuals that recordings are being taken and how they will be used such as public signage, announcements, and flyers.

Unmanned Aerial Vehicles (UAV) - Drones

We use UAVs to improve the inspection process and assist to document conditions of assets and enhance staff health and safety. They assist where an inspection may be difficult or dangerous for staff to reach or access such as the bridge structures and treetops. Images and recordings are used to determine the appropriate action required to manage the asset.

Our UAV Operating Manual and procedures regulate the use of the UAVs and ensure compliance with the Civil Aviation Safety Authority (CASA) rules that govern the use of UAV. Incidental personal or health information that is collected will be managed in accordance with this policy.

Website, Online Forums and Social Media

We use social media services (e.g. Facebook, Twitter), online forums (e.g. Shaping Banyule) and other websites to connect and interact with the community. This includes responding to customer enquiries, promoting Council facilities and services, and community consultation and feedback.

Any personal or health information collected by us via these online forums must be handled in accordance with this policy and our Social Media Policy. The information we collect via our public website can be found here Your privacy | Banyule Council.

Any commentary on our social media accounts is public. To protect the privacy of individual's, personal or health information including phone numbers or email addresses are not to be included. Public commentary may be used by us in our publications.

Principle 2 – Use and Disclosure (IPP2/HPP2)

We will only use or disclose personal or health information for the primary purpose for which it was collected. We may only use or disclose your personal information for a secondary purpose if in accordance with the Acts

or authorised or required by law to do so (e.g. where you have consented or where you would reasonably expect this to occur).

Where we disclose personal or health information about an individual as part of an investigation into unlawful activity or if it is necessary for, or on behalf of a law enforcement function then we will make a written note of that disclosure.

Feedback and Surveys

When individuals interact with us, we may use their personal information to invite them to provide feedback about their experience interacting with us to help us evaluate and improve services. Survey participation is voluntary.

Contracted Service Providers (Contractors)

We may disclose personal information to our contracted service providers who perform various services for and on behalf of the Council. These contractors are bound to provisions of the *PDP Act* and where relevant, the *HR Act* through contracts and agreements. Information provided to these contractors is limited to the information required by them to provide services on behalf of Council.

Other Agencies and Third Parties

Where authorised or required under law, we may also disclose personal and health information to the following external organisations:

- government agencies such as Department of Health and Human Services Department of Transport, Department of Health, and Australian Immunisation Register.
- law enforcement agencies, including the courts and the Victoria Police, in instances where Council is required to respond to a subpoena or provide information to assist with a Police investigation.
- government agencies to enable them to advise you of works that may impact you or your property, e.g. road constructions/closures, underground drilling, property acquisition, etc.
- Ombudsman and other regulators to assist in their investigation of a complaint received by them about Council.
- printer and mail services contractors to assist in mailing out Council correspondence.
- debt collection agencies to recover council monies.
- other agencies in the course of an investigation and defence of legal claims against Council. This includes Council's solicitors, consultants and investigators.
- organisations assisting the Council to perform statistical analysis for improving the services being delivered to the community. Where practicable and reasonable, steps will be taken to de-identify the information.
- an immediate family member of the individual, for compassionate reasons or if it is necessary to provide the appropriate care or health service to the individual, when permitted by law.
- any recipient outside Victoria, only if they are governed by substantially similar information privacy principles, or when the individual has consented to the transfer or would be likely to give it, if it was practicable to obtain that consent.
- other individuals or organisations *only* if Council believes that the disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare or a serious threat to public health, safety or welfare.

If we are frequently asked to disclose personal information to another body, we will set out our policies in a written agreement between Council and the body to which it discloses the information.

Publicly Available Information

Our public registers may contain personal information as required or permitted by law. These registers are publicly accessibly under certain circumstances, for example by inspection.

Personal Information obtained through our Customer Complaint Handling Procedure

We will not disclose any personal information provided by an individual that lodges a complaint with us to any parties who are the subject of the complaint, without the complainants prior consent, unless authorised or required by law, e.g. court subpoena.

We may also use personal information contained in complaints made to us as part of any prosecution undertaken as part of enacting law enforcement functions. We may be obliged to initiate legal proceedings because of an investigation to prosecute possible offenders.

Principle 3 – Data Quality (IPP3/HPP3)

We will take reasonable steps to make sure that the personal and health information that we collect, use or disclose, is accurate, complete and up-to-date.

You may amend any personal information you have supplied to us as outlined in IPP 6 and HPP 6.

We may need to contact an individual to confirm that the information we hold is correct to ensure we are meeting our obligations under IPP3 and HPP3.

Principle 4 – Data Security (IPP4/HPP4)

We will take all necessary steps to ensure that personal and health information is stored safely and securely. This will ensure that information held by us will be protected from misuse, loss, and unauthorised modification and disclosure. This applies regardless of the format in which the information is held.

We protect the personal and health information of individuals through several safeguards:

- policies and procedures;
- staff education and training;
- IT system and supplier procurement processes;
- physical and ICT security controls and systems.

Our Information Security Policy outlines our approach and controls in place to protect the confidentiality, integrity, and availability of our information to support Council activities and meet requirements of Part 4 of the *PDP Act*. It outlines the information security controls we have in place based on the twelve Victorian Protective Data Security Standard Elements across the following domains:

- Security Governance
- Information Security
- Personnel Security
- ICT Security
- Physical Security

Any personal or health information provided to us which is no longer necessary for Council's purposes, will be disposed of in accordance with the relevant retention and disposal authority issued by the Public Records Office Victoria.

Payment card data will be processed and handled in accordance with the Payment Card Industry Data Security Standards. Payment card details will not be stored once processed or transmitted.

Principle 5 – Openness (IPP5/HPP5)

This document and our website privacy statement (Your privacy | Banyule Council) details how we manage personal and health information. The following are other methods used to advise individuals of how personal and health information is collected and managed:

- collection notices on forms;
- CCTV signage;
- signage and other notifications at Council meetings and public events to advice audio/visual recordings or photography;
- call message recordings and verbal notification during phone calls and other interactions with staff.

On request, we will inform an individual, in general terms, of what information it holds on the individual, for what purpose this information is held and how the information is collected, held, used and disclosed. If the individual then requests further details, the individual can access their personal and health information held by Council as outlined in 'Access and Correction'.

Principle 6 – Access and Correction (IPP6/HPP6)

Individuals have a right to ask for access to their personal or health information and seek corrections. Access will be provided except in the circumstances outlined in the relevant *Act*, for example, where the information relates to legal proceedings, if it would pose a serious and imminent threat to life or health or impact the privacy of others.

Where a person requests us to correct their personal or health information, we will take reasonable steps to correct the information so that it is accurate, complete, and up-to-date in accordance with the relevant Act. We will notify the individual of the decision of the request as soon as practicable, or within 30 days of the request being received.

Personal and health information cannot be removed from records of the Council, but a correcting statement may be added.

In other circumstances a request may be required under the *Freedom of Information Act 1982* and must be made in writing stating as precisely as possible what information is required, and addressed to the:

Freedom of Information Officer
Banyule City Council
PO Box 94
GREENSBOROUGH VIC 3088

Email: foi@banyule.vic.gov.au

Further information is located on our website Freedom of information requests | Banyule Council.

Principle 7 – Unique Identifiers (IPP7/HPP7)

A unique identifier is a number or code that is assigned to an individual's record to assist with identification, e.g. a drivers licence number. We will only assign identifiers to an individual's record if it is necessary to enable us to carry out a function efficiently. An example is a unique identifier assigned to customers in our central customer database to ensure that only one name record exists for an individual.

Principle 8 – Anonymity (IPP8/HPP8)

We must, where it is lawful and practicable, give individuals the option of not identifying themselves when transacting with us.

However, as anonymity may limit our ability to process a complaint or other matter, Council reserves the right to take no action on any matter if you choose not to supply relevant personal information so that it can perform its functions.

Principle 9 – Transborder Data Flows (IPP9/HPP9)

We may transfer personal or health information outside of Victoria only if that data transfer conforms with the reasons and conditions outlined in the IPPs and HPPs where:

- the individual has provided consent;
- the recipient of the information is subject to a law, binding scheme or contract similar to the principles in the *PDP Act* and *HR Act*;
- The transfer is for the benefit of the individual and it is impracticable to obtain their consent before transfer, however it is apparent that they would likely provide consent if it was practicable to obtain.
- the disclosure is otherwise authorised by law.

Where we utilise cloud computing services outside Victoria or engage a contractor who stores data outside Victoria, all reasonable steps will be taken to ensure that the service provider or contractor will manage the personal and health information in accordance with the Victorian IPPs and HPPs. This includes ensuring that the recipient of the information is subject to laws and/or binding contractual arrangements that provide similar protections afforded by the Acts.

Principle 10 - Sensitive Information (IPP10)

We will not collect sensitive information about an individual unless the individual has consented, or when it is required or authorised by law including circumstances outlined in the *PDP Act*.

Principle 10 – Transfer or Closure of the Practice of a Health Service Provider (HPP10)

Should we discontinue the provision of a health service, a notice will be published locally advising that the service is about to be, sold, transferred or closed.

We will take reasonable steps to contact those individuals whose health information we hold to explain how we propose to deal with their information, and whether we mean to retain it or to transfer it to a new provider.

If a Council health service provider is to be sold, transferred, or amalgamated and the provider continues to provide the health service, they can elect to retain the health information. If this occurs, they will continue to hold it, in accordance with the HPPs or transfer it to a competent organisation for safe storage in Victoria until that health information is destroyed in accordance with HPP4.

Principle 11 – Making information available to another health service provider (HPP11)

If an individual requests a Council operated health service provider to make health information relating to them available to another health service provider, or that person authorises another health service provider to request the health information from Council, we will, on payment of a fee, provide a copy or written summary of the health information to that other health service provider. Council will endeavour to provide this information as soon as practicable.

6. Managing Privacy Complaints and Breaches

We are committed to the efficient and fair resolution of complaints. An individual may lodge a complaint with our Privacy Officer regarding the handling of personal and health information by Council.

Our Privacy Officer will investigate the complaint and a written response will be provided within 30 days. The complaint should include:

- what happened and how you believe your privacy has been interfered with;
- how you have been affected;
- what you would like Council to do in response to your complaint.

Complaints may be sent to:

Privacy Officer
Banyule City Council
PO Box 94
GREENSBOROUGH VIC 3088
Telephone: 9490 4222
Email: enquiries@banyule.vic.gov.au

Members of the public may make a complaint to the Office of the Victorian Information Commissioner if they believe that Council has failed to comply the IPPs, or the Health Complaints Commissioner for the HPPs. The respective Commissioner requires a complaint to have been made with the relevant organisation in the first instance.

Complaints can be directed to:

Office of the Victorian Information Commissioner
PO Box 24274
MELBOURNE VIC 3001
Telephone: 1300 006 842
Email: enquiries@ovic.vic.gov.au

Health Complaints Commissioner
Level 26, 570 Bourke Street
MELBOURNE VIC 3001
Telephone: 1300 582 113
Enquiry Form: Health Complaints Webform

7. Staff Privacy and Awareness Training

All Council staff are required to complete mandatory privacy training at induction and throughout their employment at Council to enhance their awareness about their obligations regarding the handling of personal and health information. As part of induction, they must also read and agree to abide by the Staff Code of Conduct and this policy.