Privacy & Personal Information Policy
June 2026

Greater Dandenong

Document Control

Date Created: 9 September 2002

Objective ID: A12210433

Date of Endorsement: 15 June 2026

Version No: 005

Policy Superseded by this Policy: N/A

Responsible Department: Governance Integrity Legal & Risk

Responsible Directorate: Strategy & Corporate Services

Policy Type: Mandated under the Privacy and Data Protection Act 2014

Next Review: June 2028

Document Compliance

Council acknowledges the legal responsibility to comply with the *Charter of Human Rights and Responsibilities Act 2006* and the *Equal Opportunity Act 2010*. The *Charter of Human Rights and Responsibilities Act 2006* is designed to protect the fundamental rights and freedoms of citizens. The Charter gives legal protection to 20 fundamental human rights under four key values that include freedom, respect, equality and dignity.

Greater Dandenong City Council Policies comply with the Victorian Charter of Human Rights and Responsibilities, the *Gender Equality Act 2020*, the *Climate Change Act 2017*, the Child Safe Standards contained in the *Child Wellbeing and Safety Act 2005*, (Amended) the *Privacy and Data Protection Act 2014* and the Overarching Governance Principles specified in 9(2) of the *Local Government Act 2020*.

Acknowledgment of Country

Greater Dandenong City Council acknowledges the Traditional Custodians of this land, the Bunurong People and pays respect to their Elders past and present. We recognise and respect their continuing connections to climate, Culture, Country and waters.

TABLE OF CONTENTS

1. POLICY OBJECTIVE

Greater Dandenong City Council (Council) views the protection of an individual's privacy as an integral part of its commitment towards complete accountability and integrity in all its services and programs. This policy outlines Council's management of personal and sensitive information as mandated by the *Privacy and Data Act 2014* (PDP Act) *and Health Records Act 2001 (*HR Act*).*

It is a statutory requirement that a local government organisation maintain a written policy governing the management of personal information. This policy must be made available to any individual who requests a copy.

2. BACKGROUND

Council has obligations under a broad range of Victorian legislation including responsibilities for managing and protecting the personal and health information of individuals that we collect, hold and use. These obligations are supported by our corporate and public policies and local laws.

The *PDP Act* and the *HR Act* prescribe a set of Information Privacy Principles (IPPs) and Health Privacy Principles (HPPs) outlined below that Council are required to comply with to promote and ensure the lawful, fair and responsible collection and handling of personal and health information.

Information Privacy Principles (IPPs)	Health Privacy Principles (HPPs)
Principle 1 Collection	Principle 1 Collection
Principle 2 Use and Disclosure	Principle 2 Use and Disclosure
Principle 3 Data Quality	Principle 3 Data Quality
Principle 4 Data Security	Principle 4 Data Security
Principle 5 Openness	Principle 5 Openness
Principle 6 Access and Correction	Principle 6 Access and Correction
Principle 7 Unique Identifiers	Principle 7 Unique Identifiers
Principle 8 Anonymity	Principle 8 Anonymity
Principle 9 Transborder Data Flows	Principle 9 Transborder Data Flows
Principle 10 Sensitive Information	Principle 10 Transfer or closure of the practice of a health service provider

Principle 11 Making information available to another health service provider

3. SCOPE

This policy applies to all personal and health related information collected, stored, used and disclosed by Council, including information obtained from a third party.

This policy also applies to all personal and health related information collected, stored, used and disclosed about people working for Council. This includes Councillors, Council officers, volunteers, agency staff and contracted service providers (including subcontractors) and those on work experience.

All Councillors, Council officers and third parties contracted by Council are responsible for protecting every individual's personal information collected, stored, used and disclosed by Council in accordance with the *PDP Act*, *HR Act* and this policy.

3.1 RELATIONSHIP OF THE PDP ACT TO OTHER LAWS

If a provision made by or under the PDP Act (other than Division 5, 6 or 7 of Part 3) is inconsistent with a provision made by or under any other Act, that provision in the other Act prevails to the extent of the inconsistency

3.2 GREATER DANDENONG CITY COUNCIL'S FUNCTIONS

Council's main services, functions and activities include:

- animal management
- arts and cultural programs
- business and trade development
- capital works and maintenance of parks and gardens, roads, pedestrian ways and public spaces of the city
- community health services
- elections administration
- environment and water management
- financial planning, budgets, valuations, rates and credit control
- food safety and regulation of food premises
- IT infrastructure
- land transfers and subdivisions
- library services
- marketing of the city and coordination of events
- maintenance of council-owned facilities, property and other assets

- management of parks, gardens and sporting facilities and services
- public safety
- recycling and waste management
- regulation of parking and traffic
- regulation of filming, trading and other activities in the streets
- services for children, youth, aged people and people with disabilities
- social planning and housing
- tourism
- urban planning and building regulation

4. DEFINITIONS

Personal Information	Personal information is defined in the *Privacy and Data Protection Act 2014* (PDPA) as 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.
Information Privacy Principles (IPPs)	The Information Privacy Principles (IPPs) are a set of ten principles that regulate how personal information is handled. These principles underpin the PDPA.
Sensitive Information	Sensitive information is a subset of personal information. It is defined in the PDPA as information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record.
Health Information	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.
Privacy Impact Assessment	A Privacy Impact Assessment (PIA) is a structured assessment undertaken to identify and manage privacy risks associated with

	the collection, use, disclosure, or management of personal information.
Public Registers	Public registers are documents that councils are required to make publicly available pursuant to Victorian Government legislation. These registers are: • open to inspection by members of the public or made available on Council's website. • contain information required or permitted by legislation. • may contain personal information.
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.
Third Party	A third party refers to any individual, organisation, or entity that is not part of the Council but may be engaged to perform services or functions on behalf of the Council. This includes contractors, consultants, service providers, partner agencies and other external bodies.

5. POLICY

An individual's right to decide how their personal information is handled is considered a fundamental human right under the *Charter of Human Rights and Responsibilities Act 2006*, which stipulates individuals are not subjected to unlawful or arbitrary interference in one's life and to control personal information.

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.

How Greater Dandenong City Council manages information

The following describes the way in which Greater Dandenong City Council manages personal information.

5.1 PRINCIPLE 1 – COLLECTION (IPP1/HPP1)

Council collects personal and health information necessary by lawful and fair means and not in an unreasonably intrusive way. What we collect will differ from service to service.

Council collects 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 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	
Signature	
Motor vehicle registration number	
Photograph and/or video footage	
Where you have opted in, audio recording of your phone conversations with customers service or participated on a recorded online training session	

Council will only collect sensitive or health information where consent or permission has been obtained or as required 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, Council will collect personal and health information directly from an individual. Council will only collect an individual's information from an authorised representative if the individual's consent is provided or as required by law.

All online communications with Council are protected by an industry standard 128-bit SSL encryption technology. Council employs firewall technology to help to protect internal systems and person information against intrusion from the internet.

Unsolicited information

Council may receive personal information that is not necessary for, or related to any purpose of Council, including when people send personal information to Council without Council asking for it or providing more that requested.

In circumstances where unsolicited personal information is not necessary for Council's functions, it may not be 'reasonable' to notify the individual concerned of the collection, in which case the information will simply be stored or destroyed in accordance with the *Public Records Act 1973*.

Privacy Impact Assessments

A Privacy Impact Assessment (PIA) must be conducted by the responsible Council officer where there is:

- A change to existing business operations or processes that involve personal information;
- The introduction of new or substantially changed systems or processes; and
- The proposed purchase, implementation, or use of new software applications or digital products.

Privacy Statement and Collection Notices

We will inform individuals of the matters set out in the relevant Acts via a collection notice that explains the purpose for which the information is being collected, the details of whom the information is usually disclosed to, how we will manage the information, any relevant legislation or laws requiring its collection, consequences for the individual if all or part of the information is not provided, how to access your personal information held by Council and how to make a complaint if you believe your personal information has been breached.

This notice could be provided in a form similar to below:

> *The City of Greater Dandenong is committed to complying with the **Privacy & Data Protection Act 2014 (Vic.)** and the **Health Records Act 2001**. Any personal information collected by Council will be used only for the purpose it was collected or for purposes that are related to one of our services or activities. It will be stored securely and destroyed when it is no longer required. It will not be disclosed to any third parties without your written request, unless required or authorised by law. If you do not provide the requested information, Council may be unable to deliver the necessary services. You have the right to access and correct any personal information you provide and should you have any privacy queries, feedback, or a complaint about the way your information has been handled, please contact Council on 8571 1000 or email council@cgd.vic.gov.au . For more information, including Council's **Privacy and Personal Information Policy**, please visit our website.*

Collection notices may be provided in a variety of ways, including verbally such as during phone calls, written format on physical and online forms, on our website, and signage

displayed at events including online events, such as Teams meetings where recording is taking place.

Child Safety

As a child safe organisation, Council may collect personal information about children, young people, and their families for the purposes of managing the risk of harm to children and ensuring child safety.

In cases where a child's safety is at risk and consent is not possible or appropriate, in accordance with the *Child Wellbeing and Safety Act 2005*, Council may act without consent to ensure the safety and wellbeing of a child. Council may disclose personal information to third parties without the consent of the individual or their parent/guardian, where required or authorised by law. This includes disclosures to Child Protection, the Police and the Commission of Children and Young People in cases where the child's safety or wellbeing is at risk.

Surveillance Activities

Council operates Closed Circuit Televisions (CCTV) at fixed and mobile locations across the municipality.

Council's Public Space CCTV 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*.

Victoria Police access, monitor and respond to CCTV footage in accordance with the signed Memorandum of Understanding between Council and VicPol and in accordance with the Information Privacy Principles outlined in the *Privacy and Data Protection Act 2014 (Vic).*

Members of the public can request access to recordings containing their own personal information under the *Freedom of Information Act 1982*. This will be dependant of temporary storage of records that are not required for further action.

Recorded footage will be retained for a minimum period of 30 days. Access to this material is strictly limited to evidentiary purposes or other uses permitted under applicable legislation. This includes compliance with a duly authorised subpoena, requests made under the Freedom of Information Act 1982, or as otherwise required or permitted by law.

From time to time, Council may use covert surveillance cameras for compliance purposes in accordance with the *Surveillance Devices Act 1999.*

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.

Data recorded by an activated body worn camera may be used and disclosed to a third party by the Council for the purposes of:

- incident monitoring
- providing evidence in court proceedings
- investigation of incidents where claims or complaints have been made against Authorised Officers and employees
- identification of Council employee or public safety issue
- deterrence of aggressive behaviour towards Council officers
- improved collection of evidence for prosecutions
- prosecution of incidents of occupational violence
- law enforcement

Recorded data may be shared with a third party, for example a law enforcement agency in accordance with the Information Privacy Principles outlined in the *Privacy and Data Protection Act 2014 (Vic).*

Members of the public can request access to recordings obtained by body worn cameras containing their own personal information, which is held by Council, requests must be made in accordance with the *Freedom of Information Act 1982.* This will be dependant of temporary storage of records that are not required for further action.

Members of the public can request access to recordings containing their own personal information under the *Freedom of Information Act 1982*.

Recorded footage will be retained up to 90 days, while footage required for evidentiary or other purposes will be retained in accordance with legislative requirements. Access to this material is strictly limited to evidentiary purposes or other uses permitted under applicable legislation.

Photographs, Video and Audio Recordings

We may take photographs, video or audio recordings on Council premises, from assets (e.g. 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. Recordings may also be used to investigate and respond to complaints and incidents in accordance with our Complaints 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 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.

Website, Online Forums and Social Media

Council uses social media services (e.g. Facebook, Instagram, YouTube and Twitter), online forums (e.g. Have Your Say) 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.

Council's various websites only collect or record personal information the person chooses to provide though Council's various platforms including our Contact Us section, subscription to various eNewsletters, initiatives or program updates and online applications.

Any personal or health information collected by Council via these online forums must be handled in accordance with this policy.

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.

Website Surveys

Council uses various applications, such as our community engagement platform Have Your Say, to conduct online surveys. This means the data collected online may be stored on several servers located in another country. To ensure you are fully informed on how any personal information you provide in the survey will be stored, please read the privacy policy which is contained on the online survey page, prior to participating.

Website Visits and Clickstream Data

When users visit the website, certain information is automatically collected and logged for statistical, security, and system administration purposes. This helps Council monitor website performance, identify popular and underused content, detect technical issues, and improve the user experience.

The information collected may include:

- IP address and approximate location (e.g. city level)
- Pages visited and time spent on each page
- Date and time of access
- Referring page (if the user clicked through from another site)
- Browser type and version, device type, and operating system
- Internet service provider
- Interactions with site content such as clicks, downloads, or video plays

This information is generally aggregated and anonymised. Council does not attempt to identify individuals unless required by law or to investigate improper activity.

Cookies

The website uses cookies to support functionality and improve user experience. A cookie is a small text file stored on a user's device when accessing the website. Cookies enable the website to recognise returning users, maintain secure sessions, and collect information about how the website is used.

Two types of cookies may be used:

- **Session cookies:** These exist only for the duration of a user's browsing session. They are automatically deleted once the browser is closed.
- **Persistent cookies:** These remain stored on a user's device after the browsing session ends and are deleted either manually by the user or automatically when they expire. Persistent cookies may be used to remember user preferences across sessions.

No personal information is stored within cookies used by the website. Users will not be personally identified through cookies unless legally required (for example, through a law enforcement request).

Users can manage or disable cookies through their browser settings; however, some features of the website may not function as intended if cookies are disabled.

Online Payments

Greater Dandenong City Council offers a range of secure online payment options to facilitate the payment of:

- Rates
- Infringement/fines
- Invoices or accounts
- Permit fees
- Animal registration renewal fees

Online payment options can be made via the following platforms:

- Payable
- mygreaterdandenong.com
- pay.greaterdandenong.vic.gov.au
- BPAY
- Post Billpay

These platforms utilise the Commonwealth Bank of Australia's (CBA) BPOINT payment gateway to process credit card transactions.

Council does not collect, store, or have access to any credit card information submitted through these payment services. All credit card data is securely processed by BPOINT, which is hosted in Australia and is fully compliant with the Payment Card Industry Data Security Standard (PCI DSS).

The BPOINT platform employs industry-standard encryption and secure protocols to protect users' payment information. For further details on BPOINT's security practices, please refer to the Commonwealth Bank's BPOINT website here.

Council retains only non-sensitive transaction metadata (such as payment reference numbers and confirmation details) for reconciliation, audit, and record-keeping purposes, in accordance with applicable legislation and Council's Records Management Policy.

5.2 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 relevant 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).

There are some limited exceptions that permit disclosure of sensitive information for a secondary purpose without your consent, including where it is required or authorised by or under law, or where a permitted general situation exists, like where the entity reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public.

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)

Council outsources some of its functions to third parties (contractors) who perform various services for and on behalf of the Council. These contractors are bound to the 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, Victorian Workcover Authority, Road Traffic Authority, 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 (such as 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

Under various legislation Council is required to maintain various public registers, some registers may contain personal information. These registers are publicly accessibly under certain circumstances, for example by inspection.

Where the collection of personal information is required to be included on a public register individuals will be advised through a Collection Notice at the time of collection.

Employment with Greater Dandenong City Council

Where staff have undergone a Police Checks and/or Working with Children Check, results of these checks will not be disclosed to third parties unless authorised by law and will be

disposed of in accordance with the relevant retention and disposal authority issued by the Public Records Office Victoria.

Written submissions to Council and Committee meetings

Personal information provided as part of a public submission (name and suburb) to a Council or committee meeting will be included with the published agenda papers and minutes of the meeting, which are displayed online and are available in hardcopy format for an indefinite period.

Individuals may request that their last name be withheld by selecting the appropriate privacy option (e.g., ticking a box on a form). Where such a request is made, Council will take reasonable steps to ensure these details are not published or disclosed, except where required by law or necessary for the performance of Council functions.

Personal Information obtained through our Complaints 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 complainant's 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.

5.3 PRINCIPLE 3 – DATA QUALITY (IPP3/HPP3)

Council will take reasonable steps to make sure that the personal and health information that it collects, uses or discloses, is accurate, complete and up-to-date.

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

Council 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.

5.4 PRINCIPLE 4 – DATA SECURITY (IPP4/HPP4)

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

Council protects 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.

Council's Information Security Policy establishes a framework for protecting Council information and IT systems against security attacks

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.

Personal information will be archived or destroyed in accordance with the Public Records Act 1973 and the relevant Retention and Disposal Authority from the Public Records Office Victoria.

5.5 PRINCIPLE 5 – OPENNESS (IPP5/HPP5)

The following methods are used to advise individuals of how personal and health information is collected and managed:

- privacy statements and collection notices on forms;
- CCTV signage (may be shared with Victorian Police);
- 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 Principle 6 - Access and Correction.

5.6 PRINCIPLE 6 – ACCESS AND CORRECTION (IPP6/HPP6)

Individuals can request access to information about themselves in departmental documents under *PDP Act* or *Freedom of Information Act 1982* (FOI Act). 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.

For information on how to submit an FOI request, see How to make a FOI request

Individuals may request corrections to their personal or health information by submitting a written request to Council, including sufficient details to identify the relevant record and specify the correction required.

Council will take reasonable steps to correct the information so that it is accurate, complete, and up to date in accordance with the relevant Act.

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

5.7 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 driver's licence number. Council will only assign identifiers to an individual's record if it is necessary to enable us to carry out a function efficiently.

5.8 PRINCIPLE 8 – ANONYMITY (IPP8/HPP8)

Where it is lawful and practicable, Council must offer individuals the option of remaining anonymous when transacting with us.

Before a member of Council collect personal information, they must first establish whether that particular information is required to complete their function or activity. For example, does Council need to know the name, address and contact number to action a request that a bin is on fire? Or could they remain anonymous and only provide the location of the bin?

While Council respects your right to remain anonymous, please be aware that in some cases, anonymity may limit Council's ability to fully investigate or resolve a complaint or matter. If essential personal information is not provided, Council may be constrained in the actions it can take.

5.9 PRINCIPLE 9 – TRANSBORDER DATA FLOWS (IPP9/HPP9)

The development of new technologies, such as the internal and the 'cloud' has mean that trans-border data flows between organisations have become more common (many cloud service providers are located outside Australia).

IPP9 does not prohibit the transfer of personal information outside of Victoria but it does place restrictions on when it can occur. This is because the *PDP Act* is a Victorian law and therefore the IPPs will not apply to organisations in a different state, territory or country.

Council will only transfer personal information outside of Victoria in accordance with the provisions outlined in the *PDP Act*.

Council may only transfer personal information about an individual or organisation outside of Victoria in limited circumstances, some of which include:

- the individual has provided consent;
- the disclosure is otherwise authorised by law.
- 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.

While Council uses cloud computing services based outside Victoria, it has taken all reasonable steps to ensure that the information which it transfers will not be held, used or disclosed by the host of the information inconsistently with the Victorian IPPs. It also ensures the hosts/recipients are subject to laws and/or binding contractual arrangements that provide similar protections afforded by under the *PDP Act*.

Purchase and implementation of software applications

All decisions relating to new or changed software applications will be managed on a case-by-case basis, with due regard to Council's legal obligations, risk appetite, and the protection of personal information and organisational interests.

A Council officer must conduct a Privacy Impact Assessment (PIA) prior to the purchase, configuration, implementation or material change of any software application.

The PIA must be completed early in the decision-making process and documented in accordance with Council record-keeping requirements.

Council recognises that, in limited and exceptional cases, the business benefits of a product or system may justify a departure from this policy. Any proposed departure:

- must be supported by a rigorous and proportionate PIA;
- must clearly articulate the business need and benefits;
- must identify, assess and mitigate privacy risks; and
- must demonstrate that any residual privacy risk is low and within Council's approved risk tolerance.

Where a departure from this policy is proposed, the PIA and associated risk assessment must be prepared by the relevant people leader and approved by the Governance Integrity Legal and Risk Team. Acceptance of residual privacy risk must be explicitly documented. Council will not approve solutions where privacy risks are assessed as medium or high and cannot be appropriately mitigated.

5.10 PRINCIPLE 10 – SENSITIVE INFORMATION (IPP10)

Council will not collect sensitive information about an individual unless the individual has consented, except in circumstances outlined in the *PDP Act*.

5.11 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, Council will, on payment of a fee, provide a copy or written summary of the health information to the requesting health service provider in a timely manner.

6. RESPONSIBILITIES

Managing Privacy Complaints and Breaches

If a person believes Council has wrongly collected or handled their personal information, they can write to Council.

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.

Council receives complaints through:

Email council@greaterdandenong.vic.gov.au

by mail to:
The Privacy Officer
Greater Dandenong City Council
PO Box 200
Dandenong VIC 3175

Council is committed to a quick and fair resolution of complaints. Every complaint will be investigated and complainants advised of the outcome.

If a person is unsatisfied with Council's response, they can write to the Office of the Victorian Information Commissioner (OVIC), 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.

OVIC can receive privacy complaints through:

- the online Privacy Complaint form on the OVIC's website

  by mail to:
  PO Box 24274
  MELBOURNE VIC 3001

Health Complaints Commissioner can receive privacy complaints through:

- the online Privacy Complaint form on the Health Complaints Commissioner website

  by mail to:
  Level 26, 570 Bourke Street
  MELBOURNE VIC 3001

7. REPORTING, MONITORING REVIEW AND IMPLEMENTATION

Reporting	The Manager of Governance Integrity Legal and Risk alongside the Chief People Officer is responsible for oversight. Breaches will be reported to OVIC
Monitoring	The Privacy Officer is responsible for monitoring and evaluation the performance of this policy
Review	The policy will be reviewed annually in recognition of how quickly AI Technology is evolving to reflect technological advancements, legislative changes, and organisational needs.

Stakeholder Engagement	Governance Integrity Legal and Risk, Executive Management Team, Financial Services, Chief People Officer, Chief Information Officer, Media and Communications, Child Safety, Network Services, SCC, ARC
Implementation	This policy will be made available on Council's Website. Revised Policy will be communicated to all staff via the Source.

8. BREACH OF THIS POLICY

A breach of this policy will be managed in accordance with the most current Code of Conduct, Enterprise Agreement, the Performance and Behavioural Issues Policies, and the Privacy/Data Breach Procedure and reported to OVIC.

9. REFERENCES AND RELATED DOCUMENTS

Legislation

Charter of Human Rights and Responsibilities Act 2006
Children Youth and Families Act 2005
Child Wellbeing and Safety Act 2005 (Amended)
Climate Change Act 2017
Family Violence Protection Act 2008
Freedom of Information Act 1982
Gender Equality Act 2020
Health Records Act 2001
Local Government Act 2020.
Privacy and Data Protection Act 2014
Public Records Act 1973
Surveillance Devices Act 1999
Victorian Data Sharing Act 2017

Council Related Policies, Procedures, Strategies, Protocols, Guidelines
Greater Dandenong Website – Sustainability, Climate and Energy
Access Control Policy
Artificial Intelligence (AI) Policy
Complaints Policy
Community Engagement Policy
Code of Conduct – Contractor/Representative
Information Security Policy
Child Safety & Wellbeing Policy
Working with Children Check Guidelines
Freedom of Information Policy
Mobile Device Policy
Memorandum of Understanding between Council and VicPol
Model Councillor Code of Conduct

Police Check Policy
Procurement Policy
Public Space CCTV Policy
Public Transparency Policy
Records Management Policy
Recruitment and employment privacy collection statement
Staff Code of Conduct

Other Related Policies, Procedures, Strategies, Protocols, Guidelines

Victorian Protective Data Security Framework
OVIC Guidelines to the Information Privacy Principles

Administrative Updates

It is recognised that from time to time, circumstance may change leading to the need for minor administrative changes to this document. Where an update does not materially alter this document, such a change may be made administratively. Examples include a change to the name of a Council department, the change to an existing policy or document referred to in this policy and minor updates to legislation and the like which does not have a material impact. All changes or updates which materially alter this policy must be by resolution of Council.

Date	Update