Policy and Procedure

Privacy and Data Protection

Policy Number:	2002/15	Directorate:	Corporate Development
Approval by:	CEO	Responsible Officer:	Manager – Governance
Approval Date:	3 June 2020	Version Number:	8
Review Date:	3 June 2023		

1. Purpose

The main purpose of this policy is to assist Knox City Council and staff in meeting their obligations under the Privacy and Data Protection Act 2014 for the collection, management and disclosure of personal information.

2. Context

Knox City Council (Council) believes that the responsible collection and handling of personal information is a key aspect of democratic governance and is strongly committed to protecting an individual's right to privacy. Accordingly, Council is committed to full compliance with the Information Privacy Principles contained within the Act.

About Knox City Council and our Functions

The Knox municipality is governed by nine democratically elected Councillors, each representing one of nine distinct wards. Each year the Council elects one Councillor as Mayor and one Councillor as Deputy Mayor. The primary role of Councillors is to set the vision and future direction of the Knox City Council and to advocate on behalf of the community.

The administration is made up of the Chief Executive Officer, Directors and Council staff. The primary role of the administration is to support the Council by implementing Council's goals and strategies; managing the delivery of municipal services; providing advice; and supporting the Councillors. The Administration is accountable to Council through the Chief Executive Officer.

The Local Government Act 1989 (LG Act) prescribes Council's function, including:

- advocating and promoting proposals which are in the best interests of the local community;
- planning for and providing services and facilities for the local community;
- providing and maintaining community infrastructure in the municipal district;
- undertaking strategic and land use planning for the municipal district;
- raising revenue to enable the Council to perform its functions;
- making and enforcing Local Laws;
- exercising, performing, and discharging the duties, functions, and powers of Councils under this Act and
- other Acts; and
- any other function relating to the peace, order, and good government of the municipal district.

These prescribed functions translate into the following services, events and activities offered by Council:

- advocacy
- animal management
- arts and culture programs
- asset protection permits
- building permits
- business and trade development
- capital works
- community health services
- diversity programs and events
- environment and water management
- food safety and regulation of food premises
- land transfers and subdivisions
- library services
- local law creation and enforcement
- maintenance of Council owned assets and facilities
- planning permits
- property valuations and rates
- public safety
- recycling and waste management
- regulations of parking and traffic
- services for children, youth and aged people
- regulation of filming, trading and other services on the street
- social and urban planning
- sport and leisure planning

Efficient Council Services Through Improved Data Management

Historically, Council has managed its interactions with our customers in multiple systems across multiple departments. This has resulted in duplicate, often conflicting records, and inefficient processes.

Efficient management of data across Council's entire operation is an essential part of managing a complex and diverse business; eliminating costly inefficiencies caused by data silos, and ensure that where appropriate our staff have access to accurate information.

As Council's operations become increasingly digital and data driven, it is essential that Council's data management systems also evolve. Council has implemented a comprehensive Information and Communication Technology Roadmap to drive efficiencies across Council's business, ensure we have accurate, complete and up to date information and enable simpler, clearer and more efficient customer experiences. It is of the utmost importance to Council that these systems also respect and protect the privacy of our customers.

3. Scope

This policy applies to all Councillors, officers, contractors and volunteers of Council.

This policy applies to all personal information held by Council, including information sourced by Council from third parties.

Third Party Contractors Bound by Act

Where a contractor of Council breaches the Information Privacy Principles (IPPs) the Council will be held responsible, unless the contractor has agreed to be bound by the IPPs in an enforceable contract with the Council.

For this reason all new contracts should include a provision ensuring that third party contractor, including subcontractors to them, are bound by the IPP's in the same way and to the same extent as Council. Model Terms to be used in contracts, MOU's and/or agreements have been included in section 6.13 of this policy.

To assist with compliance the contractor must be provided with a copy of this policy.

4. References

4.1 Community & Council Plan 2017-2021

- Goal 8 – We have confidence in decision making
  Strategy 8.1- Build, strengthen and promote good governance practices across government and community organisations.

4.2 Relevant Legislation

- Privacy and Data Protection Act 2014

4.3 Charter of Human Rights
- This policy has been assessed against and complies with the charter of Human Rights.

4.4 Related Council Policies
- Live Streaming of Public Meetings Policy
- Visual Surveillance Devices Policy

4.5 Related Council Procedures
- Nil

5. Definitions

Council	means Knox City Council, whether constituted before or after the commencement of this Policy.
Individual(s)	means a single person.
Community Group(s)	means a legal entity who provide services, support or activities to the Knox community.
Information Privacy Principles	Set of principles that regulate how personal information is collected, held, managed, used, disclosed or transferred by an organisation.
Personal Information	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. This can include, but is not limited to, such information as a person's: • Name, age, weight or height; • Income; • Marital status; • Education; • Home address and home number; • Employee details; or • Email address.
Primary Purpose	The purpose(s) for which an individual's personal information was collected.
Public Registers	Documents that Council is required to make publicly available pursuant to legislation. These registers are open to inspection by members of the public and contain information required or permitted by legislation.
Secondary Purpose	A purpose(s) related to the primary purpose; or where an individual would reasonably expect Council to use or disclose their personal information.
Sensitive Information	Personal information or an opinion about an individual's: • Race or ethnic origin; • Political opinions; • Membership of a political association; • Religious beliefs or affiliations; • Philosophical beliefs; • membership of a professional trade association; • membership of a trade union; • sexual preference or practice; or • criminal record

Unique Identifier	A number or code that is assigned to someone's record to assist with identification (similar to a drivers licence number).

6. Council Policy

It is the policy of Council that personal information is collected, held, managed, used, disclosed or transferred in accordance with the 10 Information Privacy Principles (IPP's) contained in the Act.

6.5 Principle 1 – Collection

The Type of Information Collected by Council

They type of personal information collected by Council will depend on the functions, services, events and activities offered by Council. The personal information Council typically collects includes, but is not limited to an individual's:

- name
- date of birth
- address
- contact information (email & phone number)
- signature
- vehicle registration number
- payment or billing information

Council staff must not collect personal information unless the information is necessary for one or more of Council's functions or activities.

Before collection occurs Council staff must have established the type of personal information they will be collecting and confirm that all personal information proposed to be collected is required for the program, service or activity they provide. Collecting personal information with no identifiable purpose is not acceptable.

Unnecessary recording of information

Sometimes, Council staff are given 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 requests some information, but people provide more information than requested.

As soon as practical after personal information is received, Council should decide whether it is relevant to what Council does. If information is not relevant, Council should not keep it in its records.

Before the information is destroyed consideration must be given to the Public Records Act 1973. If the information received would be defined as a public record under the Public Records Act Council is obligated to retain the information for a specific statutory timeframe.

Council must collect personal information only by lawful and fair means and not in an unreasonably intrusive way

In order for collection to be lawful, it must be done in accordance with the law. This means that Council must have the appropriate power to collect the information it is requesting and that there are no other laws prohibiting such collection.

Information has been collected unfairly if it was obtained by trickery, misrepresentation, deception or under duress. For example, information would have been collected by unfair means if Council knowingly accepts personal information from someone who it knows is under the mistaken belief that they have no choice but to provide said information.

Collecting personal information would be unreasonably intrusive if it involves asking questions about sensitive personal affairs, repeatedly asking for the same personal information or if the individual's personal property or space was invaded during questioning.

Informed consent for collection

Council must take reasonable steps to provide the individual with full information regarding the collection by including a collection notice at the point of collection stating:

- why Council is collecting personal information; ·
- how that information can be accessed;
- the purpose for which the information is collected; ·
- with whom the Council shares this information;
- any relevant laws; and
- the consequences for the individual if all or part of the information is not collected.

The following collection notice applies to all personal information collected by Council unless specifically stated otherwise.*Knox City Council (Council) collects personal information to enable Council to perform our statutory functions and provide services, activities and events. Council stores personal information in secure central databases and shares information amongst internal work areas (including contractors) to facilitate a more efficient customer experience across Council's business. The personal information will not be disclosed to any other external party without your consent, unless permitted or required by law. If the personal information is not collected Council may not be able to provide you with Council services, discharge our functions or keep you updated on the progress of your service request. Requests for access to and/or amendment of your personal information should be made to Council's Freedom of Information Officer. For more information, refer to Council's Privacy and Data Protection Policy.*

Direct Collection

Under normal circumstances Council must collect personal information about an individual only from that individual. This enables individuals to have some control over what is collected, by whom and for what purpose. Direct collection provides the individual with the opportunity to refuse to provide their information. It also makes it more likely that the information collected by Council is relevant, accurate and complete.

However, if Council collects personal information about an individual from someone else, Council must take all reasonable steps to ensure that individual is informed of his or her rights relating to the information collected.

Website Cookies

Council uses first-party cookies and JavaScript code to collect information about visitors to our website. Council use these applications to track how visitors interact with the website, including where they came from, what they did on the site and whether they completed any transactions on the site.

If you don't want to have cookies placed on your computer, they can be disabled through your web browser. You will need to customise each web browser you use to turn off cookie tracking. If you opt out of using cookies, you will still have access to the information and resources provided by this website however it may not function fully and your ability to browse, read, and download information may be impaired.

Council use web analytics data for statistical purposes, such as to analyse, measure, and report on data about website traffic and visits. This information helps Council understand general user trends at an aggregate level, and improve the website, content, and user experience.

Council may also use this information for security audits to protect against threats from hackers or other security purposes.

Council does not use this information to identify you or match it with any other personal information that Council may collect from you, unless required to do so as part of an internal investigation or for a law enforcement-related purpose.

Website Third Party Providers

Council uses various external applications to conduct online surveys, send newsletters, purchase tickets, book Council services and measure website use. These external providers may also collect your personal information. To ensure that you are fully informed on how any personal information is being collected it is recommended you read the privacy policy of the third party provider prior to participating. Following is a list of current third party providers used on Council's website:

- Mailchimp
- Survey Monkey
- Wufoo
- SiteImprove
- StickyTickets
- SeatAdvisor
- Readspeaker
- SmartyGrants
- Bit.ly
- Social Pinpoint
- KEYS Online
- My Family Lounge
- IMS Reserves Manager
- eTendering Portal
- Gobookings
- PageUp careers portal
- Formsexpress
- TryBooking
- Eventbrite
- Google Maps
- YouTube videos

Social Networking Sites

Council uses Facebook, Instagram and Twitter to communicate with the public. To protect your own privacy and the privacy others please do not include any personal information including phone numbers and email addresses. The social networking services will also handle your personal information for its own purposes. These sites have their own privacy policies and we recommend you read these also.

Visual Surveillance Devices (including CCTV and Body Worn Cameras)

Council owned visual surveillance devices and systems fall into three main categories:

- *Corporate Surveillance Devices and Systems* installed in public spaces, on council facilities and land. These systems are managed and monitored by council employees or contractors. This includes but is not limited to Council offices, pools, libraries, arts centres, public toilets, sporting grounds, community and child care centres, and waste management facilities;
- *Public Safety CCTV Systems* installed in public places that are monitored and managed by Victoria Police. Knox City Council has one Public Safety CCTV System located in Boronia with cameras linked to monitors at Boronia Police Station; and
- *Mobile camera devices* operated and managed by council employees or contractors. This includes body worn cameras worn by Council's enforcement staff, dash cams and aerial vehicles.

These devices are used within the community and by Council to:

- Support and implement broader crime prevention and reduction strategies;
- Enhance actual and perceived safety and security for staff and users of Council facilities;
- Discourage damage and vandalism of Council assets;
- Detect and manage any illegal activities on Council facilities and land (eg rubbish dumping or graffiti);
- Support the administration and enforcement of local laws and other legislation;

- Enhance site security and security for equipment at Council construction sites;
- Detect public safety issues;
- Support legislated responsibilities and operational business (eg aerial mapping for fire prevention);
- Monitor the use of Council land and assets such as a count of users on walking tracks or bike paths;
- Assist with traffic planning and road management such as traffic counts on local roads;
- Enhance biodiversity activities, such as wildlife monitoring and pest animal control in local bushland and parks;
- Monitor any unauthorised access to 'staff only' areas; and
- Record and promote Council events.

The use of these devises and the management of the recorded data is specified in greater detail in the Visual Surveillance Devices Policy.

6.6 – Principle 2 – Use and Disclosure

Council will take all necessary measures to prevent unauthorised access to, or disclosure of personal information.

What is use?

Use is interpreted broadly. It relates to managing personal information within the course of Council business. This includes, but is not limited to:

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

What is disclosure?

Disclosure may be interpreted as, a release, publication or revelation of personal information by Council. A disclosure can occur both within a Council and to outsiders of the Council. This includes, but is not limited to:

- 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 or sharing a computer logon, enabling unauthorised access to personal information by internal or external parties.

Council will only use personal information within Council, or disclose it outside Council:

a) for the primary purpose it was collected;

b) in accordance with legislative requirements;

c) for a secondary purpose with the consent of the individual concerned; or

d) for a secondary purpose related to the primary purpose where an individual would consider it reasonable to do so

Primary Purpose and Secondary Purpose

Where the primary purpose has been well considered at the time of collection the basic rule of IPP2 is relatively straightforward: use and disclose an individual's personal information only for the primary purpose for which it was collected.

The majority of personal information collected by Council is collected to enable Council to perform our statutory functions and provide services, activities and events. As the responsibilities for many of Council's functions and services often overlap between department's internal disclosure, and external disclosure to contracted service providers, of personal information is necessary to satisfactorily perform this primary purpose.

Secondary purposes for use and disclosure must be related (or, in the case of sensitive information, directly related) to the primary purpose of collection AND consistent with what an individual would reasonably expect. Reasonableness requires that the related secondary use or disclosure is also proper and fair, and generally not incompatible with the primary purpose of collection. When establishing 'reasonably expected' you must ask what an ordinary person, not an expert in local government would consider reasonable.

Other Departments within Council

Personal information will be disclosed internally to other work areas within Council to assist in the efficient actioning of enquiries. The personal information (contact details) contained in the single customer view may also be used to liaise with the customer in relation to the delivery of other Council services.

Contracted Service Providers

Council outsources some of its functions and services to third party contractors who perform them on Council's behalf. To enable this to occur efficiently, Council may disclose personal information we have collected about an individual to the contractor. Council will only disclose the personal information if it is necessary for the contractor to carry out its specific task.

All contracts with contracted service providers should require contractors be bound by the IPP's in the same way and to the same extent as Council. All contracted service providers should also be provided with a copy of this policy.

Legislation and Law Enforcement

The disclosure of personal information by Council in accordance with legislative requirements is not a breach of the Information Privacy Principles.

Personal information may also be contained in Council's Public Registers. Under the Local Government Act 1989, any person is entitled to inspect Council's public registers, or make a copy of them, upon payment of the relevant fee. Council maintains the following public registers containing personal information:

- Details of overseas or interstate travel undertaken in an official capacity by Councillors or any Council employee in the previous 12 months
- Register of interests kept under section 81 of the Act
- Record of persons who inspect the register of interests (limited inspection rights)
- Minutes of meetings of special committees established under section 86 of the Act and held in the previous twelve months
- Register of delegations kept under sections 87, 88 and 98 of the Act
- Register of leases entered into by Council
- Register of authorised officers appointed under section 224 of the Act
- A listing of donations and grants made by Council during the financial year including the names of recipients and the amounts received
- Register of election campaign donation returns
- Register of Planning Permits
- Register of Building Permits
- Register of all registered dogs and cats
- Written record of an assembly of Councillors

Council may also disclose personal information to law enforcement agencies, including the courts and Victoria Police, if it believes that the disclosure is reasonably necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction.

Submissions to Council

Council believes in an ongoing dialogue between the community and Council. As such Council regularly engages with individuals in the community through advisory committees as well as formal community consultation programs and activities. Personal information provided by an individual as part of an advisory committee application or community consultation will be made available to Councillors and may be included in Council reports and working documents.

Personal information provided by an individual as part of a written public submission to a Council or committee meeting may be included in the published agenda and minutes of the meeting. These documents are displayed online and available in hardcopy format for an indefinite period of time.

Any individual who addresses a public Council or committee meeting will be heard and may be seen on the live stream. Any audio and video capture on the night will be recorded. Further information on the live streaming of Council meetings can be found in Council's Live Streaming of Public Meetings Policy.

6.7 – Principle 3 - Data Quality

Council must take reasonable steps to ensure that the personal information it collects, uses or discloses, is accurate, complete and up to date.

Accurate' means that the personal information is free from error or defect. If personal information used as the basis for Council decision is incorrect the resulting Council action may unintentionally cause harm to an individual or the community.

'Complete' means having all its parts or elements. It is important that all information is complete as partial information may be misleading to Council and result in an incorrect decision that may affect an individual or the community.

'Up to date' means extending to the present time; including the latest facts. This requirement is intended to deal with situations in which subsequent information would make the existing record inaccurate. It might not always be appropriate to delete the out of date information; the Public Records Act may require its retention. In these situations it is best for Council staff to add a note detailing the information's lack of currency and add any new information.

Personal information must be accurate for the purpose it was collected. If the purpose has been completed and the records have been archived they no longer need to be monitored for data quality.

6.8 – Principle 4 – Data Security

Council will take all necessary steps to ensure that personal information is stored safely and securely. This will ensure that all personal information held by Council is protected from misuse, loss and unauthorised modification and disclosure.

Disposal of data

Council must take reasonable steps to destroy or permanently de-identify personal information that is no longer needed for any purpose. However, Council is required to comply with the Public Records Act 1973 and the relevant retention schedules. Therefore, no records should be destroyed or de-identified before seeking advice from the relevant staff member in Corporate Records.

Any destruction of records must be done in a permanent and secure manner. Council staff must not place documents containing personal information in the standard rubbish or recycling bins; the secure privacy bins must always be used.

6.9 – Principle 5 – Openness

This document and Council's website details Council's management of personal information.

On request, Council 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 information held by Council as outlined in 'Access and Correction'.

6.10 – Principle 6 – Access and Correction

Individuals have a right to ask for access to their personal information and seek corrections. Access will be provided except in the circumstances outlined in the 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 Council to correct their personal information, Council will take reasonable steps to notify the person of the decision of the request as soon as practicable.

Personal information cannot be removed from records, but a correcting statement may be added.

6.11 – Principle 7 – Unique Identifiers

IPP7 provides a safeguard against the creation of a single identifier that could be used to cross match data across various government departments.

Council does assign its own unique identifiers as necessary for the purpose of managing electronic databases, for example, through the use of unique customer numbers, but will otherwise not assign, adopt, use, disclose or require unique identifiers from individuals unless it is necessary to enable the Council to carry out any of its functions more efficiently.

Council will only use or disclose unique identifiers assigned to individuals by other organisations if:

- the individual consents to the Council doing so; or
- there are legal requirements for the Council to do so; or
- the conditions for use and disclosure set out in the Privacy and Data Protection Act 2014 are satisfied.

6.12 – Principle 8 – Anonymity

Where it is both lawful and practicable, Council will give an individual the option of not identifying themselves when supplying information or entering into transactions with it.

Anonymity may limit Council's ability to process a complaint or other matter. Therefore, if an individual chooses not to supply personal information that is necessary for the Council to perform its functions, Council reserves the right to take no further action on that matter.

6.13 – Principle 9 – Trans-border Data Flows

The development of new technologies, such as the internet and the 'cloud' has meant that transborder data flows between organisations have become more common.

The transfer of personal information outside of Victoria is not prohibited. It is however, highly restricted to when it can occur. The basic premise behind IPP 9 is that when personal information subject to the Victorian legislation travels outside Victoria, the privacy protection in the Act should travel with it.

Council may transfer personal information about an individual to another individual or organisation outside Victoria only where:

- the individual has provided consent
- disclosure is authorised by law
- the recipient of the information is subject to a law, binding scheme or contract with similar principles as the Act; or
- 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 to consent if it was practicable to obtain.

If the individual or organisation receiving information from, or on behalf of Council, is not subject to a law or binding scheme comparable to the Victorian IPPs, Council should:

- Seek consent of the affected individual; or

include specific privacy requirements in any contract, MOU or agreement it has with the recipient.

Contract, MOU or Agreement Requirements

The following Model Terms have been taken from the Office of the Information Commissioner's "Model Terms for Transborder Data Flows" document.

i. The Recipient agrees that it is bound by the Information Privacy Principles and any applicable Code of Practice with respect to any act done, or practice engaged in, by the Recipient for the purposes of this Agreement in the same way and to the same extent as Council would have been bound by them in respect of that act or practice had it been directly done or engaged in by Council.

ii. Council may disclose to any person the fact that the Recipient is a party to this Agreement for the purpose of allowing such person to assess whether Transferred Personal Information is adequately protected in the hands of the Recipient. Council may also disclose a pro forma document containing terms substantially similar to the terms of this Agreement to any person for such purpose.

iii. The Recipient agrees that it will not at any time do an act, or engage in a practice, in respect of Transferred Personal Information, that would breach an Information Privacy Principle. Specifically the Recipient:

   a) will not collect, use, disclose and otherwise handle the Transferred Personal Information for any purpose other than the primary purpose specified in this Agreement without the prior written permission of Council or the Data Subject or where required or authorised by or under Law;

   b) will not disclose the Transferred Personal Information to a person (further recipient) who is not Council;

   c) will take reasonable steps to ensure the security and quality of the Transferred Personal Information.

iv. The Recipient will immediately notify Council, in writing, of any breach or suspected breach of its obligations under this Agreement whether on the part of itself or its officers, employees, volunteers, agents or sub-contractors and of the steps taken to repair the breach.

v. The Recipient will allow and cooperate with any independent investigation of complaints by Council, OVIC or any person or body nominated by Council and provide appropriate redress to complaints for any harassing from it failure to effectively uphold the IPPs

vi. The Recipient at all times indemnifies and holds harmless Council from and against any loss, cost (including legal costs and expenses) or liability incurred or suffered by any of those indemnified arising from or in connection with any complaint, claim, suit, demand, action or proceeding by any person (including, but not limited to, any award, order or similar judgment or direction by the OVIC) where such loss or liability was caused or contributed to by the Recipient's act or omission in handling Transferred Personal Information, whether deliberate or not.

vii. Upon the termination of this Agreement, or upon the Council's written request prior to the termination of this Agreement, the Recipient will return or destroy Transferred Personal Information including all copies, in whatever form, of the Transferred Personal Information held or controlled by the Recipient.

6.14 – Principle 10 – Sensitive Information

Council will not deliberately collect sensitive information about an individual except in circumstances prescribed in the Act or in circumstances where the information is both directly pertinent and necessary to one of its functions.

Council staff must remember that a breach involving sensitive information has the potential to be even more damaging to an individual than one involving routine personal information.

Council staff must:

- only collect sensitive information if it is required either under law or if there is no reasonable practicable alternative to collecting the information for a specific function of Council.
- only use sensitive information for the purpose for which it was collected.
- when practicable, only collect the information directly from the individual.
- not use sensitive information to verify the identity of an individual.

6.15 Chief Privacy Officer

The Manager – Governance is the Chief Privacy Officer and responsible for:

- overseeing the implementation of the policy;
- monitoring the performance of the policy;
- reviewing the policy and recommending any desirable amendments; and
- periodically reporting to the Audit Committee on Council's performance pursuant to the policy.

6.16 How to Make a Complaint or Enquiry Concerning Privacy

Individuals who are concerned by Councils handling of their personal information are encouraged to contact the Chief Privacy Officer. The Chief Privacy Officer will then conduct a preliminary investigation and provide a written response within a reasonable timeframe. Complaints or enquiries to the Chief Privacy Officer should be sent to:

Chief Privacy Officer

511 Burwood Hwy

Wantirna South VIC 3152

Email: knoxcc@knox.vic.gov.au

Website: www.knox.vic.gov.au

Alternatively, complaints or enquiries may be made directly to the Office of the Victorian Information Commissioner. It should be noted that the Commissioner may decline to hear the complaint if the individual has not yet contacted Council with their concerns.

Complaints to the Office of the Victorian Information Commissioner (OVIC) should be sent to:

Office of the Victorian Information Commissioner

PO Box 24274

Melbourne VIC 3001

Email: enquiries@ovic.vic.gov.au

Website: www.ovic.vic.gov.au

Complaints must be lodged within 6 months from the time the complainant first became aware of the conduct or misconduct. At all times the contents of the complaint will be kept confidential.

Employees who are in breach of this policy may be subject to disciplinary action, performance management and review. Serious breaches may result in termination of employment, in accordance with the Staff Discipline policy and procedure.

6.17 How Council will handle a privacy complaint

If a complaint is received, Knox City Council will be proactive in dealing with the potential privacy breach and its consequences.

There are four key steps that will be taken by Council once a complaint or enquiry has been received or once it becomes aware that a privacy breach has occurred. These stages are:

1. Contain the breach and conduct a preliminary assessment
2. Evaluate the risks associated with the breach
3. Remediate and notify affected parties (if required)
4. Review the cause of the breach and Council's response. This includes taking steps to improve practices and lessen the likelihood of future breaches.

Once an officer becomes aware a privacy breach has occurred they must notify their team leader or coordinator and take immediate action to contain the breach. This action could involve recovering the records, stopping the unauthorised practice or ensuring that the physical location in secure.

The team leader or coordinator must contact one of the Privacy Officers in Governance who will assist the breach investigation and assist the officer in completing the above key steps.

7. Administrative Updates

From time to time, circumstances may change leading to the need for minor administrative changes to this policy. Where an update does not materially alter this policy, such a change may be made administratively. Examples of minor administrative changes include changes to names of Council departments or positions, change to names of Federal or State Government departments or a minor amendment to legislation that does not have material impact. Where any change or update may materially change the intent of this policy, it must be considered by Council.