POLICY

Privacy and Data Protection

Policy Number:	2002/15	**Directorate:**	Customer and Performance
Approval by:	Chief Executive Officer	**Responsible Officer:**	Manager Governance and Risk
Approval Date:	21/03/2025	**Version Number:**	10
Review Date:	3 Years from Meeting Date		

1. Purpose

The main purpose of this policy and procedure is to assist Knox City Council (Council) to meet its obligations under the Privacy and Data Protection Act 2014 for the collection, management, use and disclosure of personal information.

It is also a statement of Council's ongoing commitment to appropriately manage the information that is disclosed to Council staff during all Council operations.

2. Context

Council believes that the responsible collection and handling of personal information is a key aspect of good governance and is strongly committed to protecting an individual's right to privacy. Accordingly, Council is committed to full compliance with its obligations under the *Privacy and Data Protection Act 2014 (Vic)*.

3. Scope

3.1 Inclusions

This policy applies to all:

- Councillors, Council staff, contractors and volunteers of Council.
- personal information held by Council, and includes information we have collected:
  - about a person through any of Council's public interfaces.
  - from a person.
  - information sourced by Council from third parties.
  - abouta person.

The above includes information, regardless of the format, collected on forms, in person, in correspondence, over the telephone or via our website.

3.2 Exemptions

Certain information is exempt from the provisions of the *Privacy & Data Protection Act 2014*. For instance:

- documents on the website, which by their nature cannot be deemed to be private.
- information used for law enforcement is exempt due to its required use for legal purposes.

The privacy legislation outlined in this policy is in addition to existing legislative obligations that regulate the way Knox City Council handles personal Information. Therefore, the requirements under the *Freedom of Information Act 1982* and the *Local Government Act 2020* also apply.

While some unpublished documents or information held by Council can be routinely accessed upon request, formal requests for access to certain documents may still need to be made in accordance with the Freedom of Information Act 1982.

These Freedom of information processes also apply to Councillors, Council staff, contractors and volunteers seeking access to information or documents which is not readily accessible or routinely shared with them during the normal course of their duties.

4. References

4.1 Community & Council Plan 2021-2025

- Ensure our processes are transparent and decisions are accountable.

4.2 Relevant Legislation

- *Local Government Act 2020*
- *Local Government (Governance and Integrity) Regulations 2020*
- *Privacy and Data Protection Act 2014*
- *Public Records Act 1973*
- *Freedom of Information Act 1982*
- *Child Wellbeing and Safety Act 2005*
- *Child Wellbeing and Safety (Information Sharing) Regulations 2018*

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

- Visual Surveillance Devices Policy Information Management Security Policy
- Records Management Policy
- Health Records Policy
- Live Streaming of Public Meetings Policy
- Public Transparency Policy

4.5 Related Council Procedures

- Privacy and Data Protection Guidelines
- Data Breach Process

5. Definitions

Detail any definitions within the policy.

Council	means Knox City Council, whether constituted before or after the commencement of this Policy.
Community Group(s)	means a legal entity who provide services, support or activities to the Knox community.
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
Individual(s)	means a resident(s) of the Knox Municipality and any individual who may contact Knox City Council to utilise their functions.
Information Privacy Principles	means the set of principles prescribed in the Privacy and Data Protection Act 2014 that regulate how personal information is collected, held, managed, used, disclosed or transferred by an organisation.
Invasive collection	means information has been collected after probing into sensitive personal matters. Example: Collecting personal information becomes invasive if it involves probing into sensitive personal matters, repeatedly requesting the same personal information or invading an individual's personal property or space during questioning

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. 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 • telephone number (home and mobile) • employee details • email address
Primary Purpose	means the purpose(s) for which an individual's personal information was collected.
Public Registers	means the 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	means 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	means 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 • criminal record
The Act	Unless the context indicates otherwise, means the Privacy and Data Protection Act 2014
Unfair collection	means information that has been obtained by trickery, misrepresentation, deception or under duress. Example: requiring a resident to provide sensitive personal details (e.g., medical history) to access services where health information is not a relevant consideration (eg hard rubbish collections)
Unique Identifier	mean a number or code that is assigned to someone's record to assist with identification (similar to a drivers licence, tax file number or medicare number).

Use	Interpreted broadly, use 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 or AI model

6. Council Policy

Council's will manage personal information in accordance with the 10 Information Privacy Principles (IPPs). The 10 IPPs contained in the Privacy and Data Protection Act 2014 (Vic) are listed below:

- 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 - Trans Border Data Flows
- Principle 10 - Sensitive Information

The following sections of this policy are a summary of Council's consideration of the IPPs and how they are applied to Council's functions, services, events, and activities.

6.1 Principle 1 – Collection

6.1.1 Before collection

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.

Under sections 10(1) and 10(2) of the *Local Government Act 2020*, Council has the power do all thing necessary or convenient in connection with the performance of its role (subject to limitations imposed by this or other Acts).

Council will only collect information to support the functions, services, events and activities it provides. Council is committed to supporting staff to understand how to collect that information.

All new staff members are required to complete a compulsory induction program initially and ongoing refresher training. It is important that Council educates staff that:

- unfair and invasive collection is unacceptable and will not be tolerated.
- It is not acceptable to collect personal information with no identifiable purpose.

6.1.2 The Type of Information Collected by Council

The personal information that Council collects varies based on its functions, services, events and activities. Council will only collect personal information necessary for one or more of its core functions

or activities. This information typically includes but is not limited to:

- name
- address (residential, postal and email)
- telephone number (work, home and mobile)
- date of birth
- signature
- occupation
- medicare number
- credit card and bank account numbers
- motor vehicle registration number
- photograph and/ or video footage
- audio recordings of your phone calls to customer service
- Caller ID information from phone calls (including Voice Over Internet Protocol [VoIP] calling)

Council may collect your personal information for purposes including, but not limited to, the following:

- To contact you where it is necessary in order to provide services requested by you, such as obtaining a residential parking permit via our public interfaces.
- As part of our commitment to customer service, we may periodically invite you to provide feedback about your experience via a survey. Any survey is voluntary and you do not have to participate.
- For Council or our contracted service providers to contact you where it is necessary to resolve issues relating to Council services or functions which you have brought to our attention. For instance, contacting you in response to your report of a fallen tree branch.
- To contact you prior to a Council or Committee meeting to confirm your attendance and/or advise you of any changes to the meeting details where you have made a submission for consideration.
- To supply you with material concerning Council initiatives and programs where you have supplied personal information to Council for this purpose. For instance, where you have opted to be included on a mailing list for a Council publication via our public interfaces.
- To facilitate the collection of Council fees and charges. For instance, we will use your name and address details to forward rate notices.
- To enable payment for Council provided goods and services.
- To enable Council to undertake its law enforcement functions. For instance, Council collects information about you from various Road Traffic Authorities to process parking infringement notices.
- To aid community safety. For instance, Council collects images via closed circuit television cameras which are located throughout our municipality.
- To record/receive ideas, questions, complaints, and compliments from members of the public. The public is encouraged to join the open conversation and debate via Council's social media accounts/participation platforms but is expected to participate in a respectful manner.
- To ensure that Council has sufficient details to verify a customer's identity, and enable the provision of services, and appropriate and secure record keeping in a lawful, efficient and secure manner.

From time-to-time Council may collect information about an individual from a source other than that individual. Examples include but are not limited to:

- a third party may provide Council with address change notification, which is used to update customer records.
- Council may obtain demographic or customer interests' information, which is used for planning purposes and understanding customer consumption patterns and behaviour.

6.1.3 Informed consent for collection

Council must take reasonable steps to ensure individuals are fully informed about the collection process by providing a notice at the collection point stating:

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

Council's standard collection notice applies to all personal information collected by Council unless specifically stated otherwise. The standard collection notice is as follows:

> *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.*

6.1.4 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 their rights relating to the information collected.

6.1.5 Collection by Artificial Intelligence

Artificial Intelligence (AI) is a way for computers to perform tasks that humans normally would. While the full extent of the use of AI is still to be realised, Council is already using it to help increase efficiency. Some of the uses may include but are not limited to:

- identifying objects or hazards using video
- making predictions
- translating language
- collecting information
- processing very large amounts of information

Before a decision is made to use artificial intelligence (AI) solutions to collect or use personal information, or outsource work to a third party who uses AI, a Privacy Impact Assessment (PIA) must be completed along with a security risk assessment. These assessments will help Council to ensure compliance with the IPPs and to identify privacy risks that might arise from either the outsourcing arrangement or the use of AI. These assessments should be reviewed throughout the term of the arrangement.

6.1.6 Third Party Contractors Bound by Act

Council provides some services through third party contractors. This may result in Council collecting personal information via contractors so Council requires its contractors to comply with the Act. 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 should be used in contracts, Memorandums of Understanding and/or agreements. To assist with compliance the contractor must be provided with a copy of this policy.

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

6.1.7 Third Party Providers

6.1.8 Council uses several external applications for tasks such as online surveys, newsletter distribution, ticket purchases, booking Council services, and measuring website usage. These external providers may collect personal information. Council ensures that third-party applications have accessible privacy policies for users to review before engaging with them, so that the collection and use of data is clearly understood. These privacy policies are available within the applications themselves or through the privacy page on Council's website.Website Cookies

Council uses first-party cookies and JavaScript code to collect information about visitors to our website. These tools track visitor interactions such as their origin, activities on the site, and any transactions completed on the site.

Web Analytics	
Council uses it for	Council does not use it to
• statistical purposes, to help understand overall user trends and enhance user experience • security audits to mitigate potential threats.	• identify you • link it with other collected personal information, except when necessary for internal investigations or law enforcement purposes.

If you prefer not to have cookies stored on your device, you can disable them through your web browser settings. However, this might affect the website's functionality, potentially impairing your ability to access and use certain features. Furthermore, in the case of online interactions, for security logging purposes we may capture users IP (Internet Protocol) address, what the IP address accessed on the site/system (eg website, eservices, etc).

6.1.9 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.

6.1.10 Visual Surveillance Devices (including CCTV and Body Worn Cameras)

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

- Corporate Surveillance Devices and Systems
- Public Safety CCTV Systems
- Mobile camera devices including body worn cameras

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

6.1.11 Unnecessary recording of information

At times, Council staff receive personal information that is unrelated to or unnecessary for any Council business. 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.

Upon receiving personal information, Council will assess the information and the relevance to the activity, program or service it was provided for. Council will manage this information as per the requirements of the *Public Records Act 1973.*

6.2 Principle 2 – Use and Disclosure

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

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.

6.2.1 Primary Purpose and Secondary Purpose

The rule of IPP2 is relatively straightforward: use and disclose an individual's personal information only for the primary purpose for which it was collected.

Most personal information collected by Council is collected to enable Council to perform statutory functions and provide services, activities and events.

Sometimes Council will have to share this information with others because the responsibilities for many of Council's functions and services often overlap between internal departments and external contracted service providers. Sharing will occur when it is necessary to satisfactorily manage an enquiry or request, or discharge a Council function.

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.

6.2.2 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.

6.2.3 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.

6.2.4 Child Information Sharing Scheme

Council is prescribed as an information sharing entity under the Child Wellbeing and Safety (Information Sharing) Regulations 2018 for their Maternal Child and Health function.

The Child Information Sharing Scheme operates under Part 6A and 7A of the Child Wellbeing and Safety Act 2005 (Vic) which allows Council to share confidential information to support child wellbeing. To find out more about this scheme, refer to the Health Records Policy.

6.2.5 Law Enforcement

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

6.2.6 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 is committed to creating opportunities for 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.

6.2.7 Use of Data with Artificial Intelligence

Personal information may be used by artificial intelligence (AI) systems and applications in different ways and for different purposes.

Similarly to collection by humans, where AI systems and applications are not using personal information for the primary purpose, the use for a secondary purpose may be authorised where it is related to the primary purpose and would be reasonably expected by individuals.

Council will treat the information collected in the same way as if it was collected by humans and consider legislative and regulatory requirements.

Unless specifically authorised, staff must not input personal information collected by Council into AI systems (for example, publicly accessible services such as Chat GPT, Microsoft CoPilot in Edge Browser).

6.3 Principle 3 - Data Quality

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

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.

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, however it may not be appropriate to delete out-of-date information as 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.

Where artificial intelligence (AI) solutions are used to cleanse data, the use of AI solutions must be informed by a privacy impact assessment.

6.4 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.

6.4.1 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.

6.5 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'.

6.6 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.

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.

6.7 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.

6.8 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 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.

6.8.1 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 and may be used for Contracts, Memorandums of Understanding (MOU) or Agreement requirements:

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 subcontractors 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.*

6.9 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.

6.9.1 Chief Privacy Officer

The Manager Governance and Risk 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 and Risk Committee on Council's performance pursuant to the Policy.

6.9.2 How to Make a Complaint or Enquiry Concerning Privacy

Individuals who are concerned by Council's 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.

6.9.3 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 on approval of the Director Customer and Performance. 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 the Chief Executive Officer .