CITY OF ADELAIDE

# Privacy Policy

*September 2025* *Council* *non-legislative*

**PURPOSE**

The purpose of this Policy is to establish the basis for the practices and procedures of the City of Adelaide (the **Council**) in relation to the collection, use, storage and disclosure of personal information. The provisions of the *Privacy Act 1988* (Cth) (the **Privacy Act**) do not apply to this Council or any other South Australian Council, however it is the intention of the Council that its policies and practices in relation to privacy should be, so far as is reasonably practicable, consistent with the Privacy Principles set out in the Privacy Act. Council is bound by the Privacy (Tax File Number) Rule 2015 issued under the Privacy Act. This Privacy Policy (the **Policy**) is, therefore, a measure which is intended to promote what the Council considers to be "best practice".

**STATEMENT**

## Privacy Governance Approach

Privacy governance is an integral part of service provisions and is the responsibility of governing authorities, senior management, legal, information management and privacy officers. While effective governance and leadership are essential, collaboration across the Council is a critical factor in achieving a robust privacy program.

This Privacy Governance Approach (the **Approach**) can be used and incorporated into existing governance mechanisms within Council. Oversight and accountability for privacy and the management of personal information can be achieved through existing processes and risk management oversight processes.

The Approach, as articulated within this Policy, exists to provide guidance and help local government agencies to comply by:

- Better understanding of privacy risks and opportunities, including the potential use and implementation of new data-driven technologies (e.g. artificial intelligence (AI)).
- Addressing roles and responsibilities throughout the agency in relation to privacy management.
- Keeping the interests of the individual paramount in a user centric manner.
- Embedding a proactive approach to privacy management and privacy-by-design throughout the agency.
- Implementing robust personal information lifecycles – that is the collection, use, security and disposal of personal information.
- Prompt notification in the event of an eligible data breach and affected individuals where there is unauthorised access to or unauthorised disclosure of, or a loss of personal information that is likely to result in serious harm.
- Ensuring there are up-to-date privacy policies and procedures.
- Ensuring there is privacy-by-default and a transparent and open governance approach whatever the business practice or technology involved.
- Embedding a culture of protecting personal information within the agency.

## Privacy Principles

The Privacy Act contains thirteen privacy principles which govern standards, rights, and obligations regarding the collection, use, and disclosure of personal information, the organisation's governance and accountability, integrity, and individual rights.

The Policy refers to and incorporates these privacy principles, which are as follows:

- Open and transparent management of personal information
- Anonymity and pseudonymity
- Collection of solicited personal information
- Dealing with unsolicited personal information
- Notification of the collection of personal information
- Use or disclosure of personal information
- Direct marketing
- Cross-border disclosure of personal information
- Adoption, use or disclosure of government related identifiers
- Quality of personal information
- Security of personal information
- Access to personal information
- Correction of personal information

## Roles and Responsibilities

While the mix of roles and responsibilities will vary depending on the circumstances, effective privacy implementation includes the following key functions and roles:

- **Privacy Officer**: Associate Director Governance & Strategy – responsible for ensuring Council protects the privacy of individual's personal information. This includes overseeing the implementation of privacy guidelines, and handling privacy-related enquiries and complaints.

- **Information Management** and **Cybersecurity staff** – responsible for identifying and monitoring data privacy breaches.

- **Associate Directors** – responsible for considering privacy issues, implementing thePolicy and completing the Privacy Impact Assessment Tool as well as managing the handling of personal information across their business unit activities (projects, programs and service delivery).

- **People** – responsible for inducting and training staff on the Policy and procedures via online training.

- **CoA employees** – comply with the Policy and procedures set out by Council.

- **Governance & Strategy Program** – responsible for ensuring management of the Policy, compliance, reporting and providing advice about Council's privacy obligations and needs for flexibility.

For Council to achieve a robust privacy program, collaboration is essential across staff with key roles and responsibilities for privacy, information security and records.

## Collection of Personal Information

The Council may collect and hold personal information about current, potential and former

employees, customers, contractors and/or suppliers of the Council, and other persons that the Council has dealings within the course of conducting its functions and objectives.

The personal information that may be collected will depend on the particular purpose for which it is collected (see section 4 "Use and disclosure of personal information"), and may include:

- Telephone numbers
- Name and addresses (postal, residential and e-mail addresses)
- Age and/or date of birth
- Property ownership and/or occupier details
- Details of resident's/ratepayer's spouse or partner
- Development applications, including plans or specifications of buildings
- Pet ownership
- Electoral roll details
- Pensioner / concession information
- Payment history
- Financial, rental or income details
- Details of land valuation
- Preferred addresses and methods of contacts
- Details of employment
- Insurance details
- Records of Council's communications or dealings with an individual including any complaints, incidents, requests or queries
- Information that an individual posts to the Council's Sites, Apps or Channels
- Information collected when an individual accesses the Council's Sites, Apps or Channels, including device ID, device type, IP address, geo-location, computer and connection information, referral URL, statistics on page views, traffic to and from the Council's Sites, Apps and Channels
- For job applicants, contractors and suppliers, information about their occupation, employment history, education and suitability for the role or relationships [including criminal history, social media profiles and whether they hold any licences/permits or police clearances required for the role]
- CCTV footage of your image and recording your voice from any of the Council's premises or broader council area
- Images and your voice from body worn cameras
- Photographs and videos of your image and/or voice from any events or functions organised by the Council or held within its premises or broader Council area

The Council will take reasonable steps to inform the individual whose personal information it collects:

- of the purpose(s) for which the personal information is being collected;
- if the collection of the information is authorised or required by law, that the collection is so authorised or required;
- in general terms, of its usual practices with respect to the use and disclosure of personal information of the kind collected.

Council will take reasonable steps to ensure that personal information it collects is relevant to the purpose(s) of collection and is up to date and complete.

Council will take reasonable steps to ensure that its collection of personal information does not

unreasonably intrude upon an individual's personal affairs.

Council may collect information concerning individuals from a number of private and public sector agencies, which may include, but are not limited to Transport SA, the State Electoral Office, Office of the Valuer General, SA Water, Telstra and from individuals or publicly available websites or sources.

If Council has been provided information from a third party about another person, the third-party warrants that they have the person's permission to do so.

## Collection of Sensitive Information

Council may collect sensitive information where relevant to the particular purpose for which it is collected. For example, for current, potential and former employees and/or contractors, the Council may collect health and medical information, diversity information (eg ethnicity, gender etc) and/or information about their criminal history or police clearances (as may be required for their role/engagement).

Council may also collect sensitive information from individuals for the purpose of health and safety compliance established by the Australian Government, and the South Australia Government to enable the Council to make informed health and safety decisions.

Photographs or videos may contain sensitive information about individuals if any of the following information is apparent:

- their racial or ethnic origin;
- their political opinions or associations;
- their religious or philosophical beliefs;
- their trade union membership or associations;
- their sexual orientation or practices;
- their criminal record; or
- their health information.

Council will not collect sensitive information about an individual unless:

- the individual has implied consent, and the collection is reasonably necessary for Council's functions or activities;
- the collection is required or permitted by law;
- the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any person;
- the collection is necessary for the establishment, exercise, or defence of a legal or equitable claim.

## Maintenance and Storage of Personal information

Council will retain an individual's personal information for as long as required to fulfil the purpose for which it was collected, unless a longer retention period is required for the purpose of discharging its legal, accounting and reporting requirements. Council may disclose some personal information to an offshore third-party cloud computing services provider. In this event, Council will take adequate and reasonable steps to assure appropriate data security.

Council will take reasonable steps to:

- protect the personal information it holds from misuse and loss and from unauthorised access,

modification, or disclosure, for example through the use of technical and physical security measures, including restricting access to electronic records through technical access restrictions;
- maintain its record keeping systems to ensure that all personal information collected is up to date, accurate and complete as far as reasonably practicable; and
- ensure that any person who, on behalf of the Council, uses or discloses personal information held by the Council has appropriate authorisation to do so.

Council will promptly and diligently comply with its legal obligations in the event of a data breach involving Tax File Number (TFN) information.

## Use and Disclosure of Personal Information

In general, the Council collects, holds, uses and discloses personal information for the following purposes:
- to verify the identity and communicate with individuals;
- to provide and market the Council's services;
- to respond to any feedback, queries or complaints;
- to help the Council to operate, protect, manage, improve, conduct and develop its services, and its customers' experiences, for example, by performing analytics and conducting research;
- to maintain and administer records;
- to process, administer, collect payments from or make payments to individuals, and if applicable, make appropriate taxation deductions;
- to assess suitability of potential employees or contractors;
- to assess performance of current employees or contractors;
- to ensure health and safety on the Council's premises and in the broader council area;
- to provide joint marketing initiatives with other service providers;
- to perform data analysis and/or market research;
- to comply with the Council's reporting and other legal obligations;
- to communicate and promote the Council's activities, as well as progress on key strategic projects and initiatives within the Council area;

As otherwise may be required for the general management and conduct of the Council's legislative functions. CCTV footage specifically may be used for the following purposes:
- detecting and deterring unauthorised access to, and criminal behaviour on the Council premises/in the Council area;
- monitoring the safety and security of the Council's customers, employees, contractors, and suppliers, and completing incidents investigations;
- investigating the actions of staff, contractors and members of the public where an allegation of serious misconduct is identified by Council to have occurred in a Council workplace.

Photographs and videos taken at Council events or functions or held within the Council's premises or broader Council area may be used to:
- publicise and promote activities of the Council, or activities of third parties which are conducted within the Council area; and
- communicate Council initiatives to our residents, as well as the general public.

Where the Council collects personal information for a particular purpose, Council may use and disclose personal information for the purpose for which it was collected, unless specifically requested by the individual not to use the information for that purpose. Any other related purpose

(or directly related, for sensitive information) and otherwise where permitted or required by law or with the individual's implied consent. Council reserves the right to use or disclose the individual's personal information if it is reasonably believed that:

- use or disclosure is reasonably necessary to prevent or lessen a serious or imminent threat to the life or health of the individual concerned or another person;
- use or disclosure is reasonably necessary for the enforcement of the criminal law or of laws imposing a pecuniary penalty.

Direct Marketing:

- Council may use an individual's personal information to contact them from time to time whether by email, phone or SMS, to tell them about services, offers, promotions and events;
- if an individual does not want Council to contact them for these purposes, they can withdraw implied consent and advise at any time by unsubscribing from the mailing list by clicking on the link in the marketing communication or contacting the Customer Services (at the contact details below).

## Disclosure to Third Parties

The Council may disclose personal information to third parties contracted by the Council to provide advice or services for the purpose of assisting the Council in providing benefits to individuals (for example: State Electoral Office, Office of the Valuer General, insurers, legal service providers, photographers or videographers).

The Council will take reasonable steps to contract only with third party service providers that are subject to the provisions of the *Privacy Act 1988* and the Australian Privacy Principles.

## Integrity and Alteration of Personal Information

Council relies on individuals providing personal information that is accurate, complete and up to date. It is the responsibility of individuals to provide the Council with details of any changes to their personal information as soon as reasonably practicable following such change. Council does not accept responsibility to individuals for any loss or damage arising from reliance on personal information provided to them by Council.

An individual may apply to the Council, in a form determined by the Council, to have their personal information amended so that it is accurate, relevant, complete, up-to-date, and not misleading. If Council is satisfied that the personal information held by it is inaccurate, incomplete, or out of date, Council will take reasonable steps to amend its records accordingly.

Where the Council, on reasonable grounds, decides not to amend a resident's or ratepayer's personal information in the manner requested in the application, the Council will inform the individual of its decision and the reasons for refusing to make the requested amendments. For example, an individual may have signed a talent release form, allowing photos or videos of them to be used without further consultation with the individuals. If requested by a resident or ratepayer, the Council will take reasonable steps to attach to a record containing that individual's personal information a statement provided by that individual of the correction, deletion or addition sought.

## Access to Personal Information

A person who wishes to access personal information held by the Council must make a written application to the Freedom of Information Officer. An applicant will be required to pay an

application fee as determined by the *Freedom of Information Act 1991*.

Subject to the provisions of this legislation, the Council may grant or refuse access to personal information as it deems fit.

The Council recognises that there are certain documents, which may contain personal information, that the Council is legislatively required to make available for access by members of the public. An application to access personal information will be dealt with within 30 days of receipt of the request. In certain circumstances, an applicant may be required to satisfy Council staff as to his or her identity.

Personal information may be released to others if requested under the *Freedom of Information Act 1991*, however, in accordance with this legislation, an individual will be consulted to obtain their opinion on release of the information. Should it be determined the information will be released against the views of the individual, they have the right to request a review of the decision, on payment of the prescribed fee, prior to the information being released.

## Suppression of Personal Information

An individual's name or address may be suppressed from the Council's Assessment Record and Voters Roll where the Chief Executive Officer is satisfied that inclusion of the name or address on the Assessment Record and/or Voters Roll would place at risk the personal safety of that individual, a member of their family, or any other person.

Enquiries regarding the suppression of personal information should be directed to Customer Services staff at the Customer Service Centre in the first instance.

## Privacy Impact Assessment Methodology

The Privacy Impact Assessment Methodology allows decision-makers to systematically identify risks to privacy and develop appropriate solutions. The process is an on-going cycle with the following steps:

- Framing the business objectives: describe the functionality of the project/service and describe the business needs and benefits it serves.
- Framing privacy governance: it is important to know what levels of legal, institutional, or circumstantial requirements are applicable.
- Assessing the system design: identify and catalogue the inputs for the risk analysis (these inputs are the data actions performed by the system, the personal information processed by each data action).
- Assess privacy risks: determine the privacy risk of a particular data action (likelihood that a data action will be problematic and its impact). Assess the likelihood and impact, then calculate and priortise the risk.
- Selecting privacy controls: support the selection of controls that mitigate the risks identified.
- Monitoring change.

A Privacy Impact Assessment (PIA) identifies the impact that a project may have on individuals' privacy and sets out recommendations for managing, minimising, or eliminating the impact. The assessment is an important component in protecting privacy and should be part of the overall risk management and planning when considering a project that will include the privacy of the Council's

customers.

Privacy issues that are not properly addressed can impact on the community's trust of Council and undermine a project's success. For any project that will involve the handling of personal information the Council should consider undertaking a Privacy Impact Assessment (PIA). Under the Privacy Act, information does not always have to include details such as the individual's name to qualify as personal information. It may include other information that can identify an individual or allow their identity to be determined.

A threshold assessment should be performed to determine if the project is considered to be a high privacy risk project:

- Identify whether your project involves new or changed ways of handling personal information, and Screen for factors that may point to the potential for a high privacy risk project.
- If your project has the potential of being high privacy risk, it is recommended to complete a PIA as part of the project planning stage using the Privacy Impact Assessment Tool.

## Cookies and links to other IT sites

To improve the Council's Sites, Apps and advertising, and to help us better understand browsing behaviour, when an individual uses the Council's Sites and Apps, the Council may use website measurement software and other analytics tools and services (including Google Analytics) to gather information such as traffic patterns, mouse click activity, IP addresses, and any other information the individual may provide through use of the Sites or Apps. The Council may also use analytics tools available on its Channels. This information is aggregated and anonymised so that the individual cannot be identified.

Like many other websites on the internet, the Council may use 'cookies' to store and track information about an individual when they are using its Sites or Apps. A cookie is a data file that is sent to an individual's browser from a web server and stored on the individual's computer (or other device), then sent back to the server by the individual's browser each time they access certain sections of the Council's Sites or Apps.

This information helps the Council to remember the individual's preferences and can help to provide them with a tailored experience and customised content and material on the Council's Site and Apps and subsequent websites they may visit. This information may be retained in an anonymous or aggregated form after the Council has erased personal information that identifies individuals from its systems.

The Council also uses cookies to target online advertising to site users. This enables the Council and its partners to target relevant advertising content to individuals. The Council may provide data in an anonymous form from cookies to third parties to enable those third parties to promote the City of Adelaide via online advertising.

Website users can choose to disable cookies via their device's website browser settings. However, if they choose to reject cookies, they may not be able to use or access some features of the services that Council offers.

The Council may have links or references to other websites from our Site and Apps. This policy does not apply to those third-party websites, and the Council takes no responsibility for any information collected by such third parties.

## Queries, comments & complaints

Any individual who has any concerns regarding how the Council handles personal information or requires further information can contact the Customer Services staff at the Customer Service Centre in the first instance.

If the individual's concerns cannot be satisfied, they may lodge a formal complaint, under the Corporate Complaint Handling Guideline.

## Application of this document

This Policy applies to all people with access to Council information, including but not limited to systems and stores (computer-based or otherwise) including:

- Council staff
- Council Members
- Volunteers
- Work experience placements
- Trainees
- Independent contractors and consultants

**OTHER USEFUL DOCUMENTS**

## Related documents

- Code of Conduct for CoA Employees
- Council Members Allowances and Benefits Policy

## Relevant legislation

- *Local Government Act 1999* (SA)
- *Privacy Act 1988* (Cth)
- Information Privacy Principles
- *Freedom of Information Act 1991* (SA)

Threshold Privacy Assessment - SA Health Report Template - Blue and White - Helix Position A

**GLOSSARY**

Throughout this Policy, the below terms have been used and are defined as:

**Access** means providing to an individual, information about himself or herself that is held by the Council. This may include allowing that individual to inspect personal information or to obtain a copy.

**Assessment Record** means Council's property listing showing owners and occupiers

**Collection** means gathering, acquiring, or obtaining personal information from any source and by any means, including information that the Council has come across by accident or has not asked for.

**Implied consent** means voluntary agreement to some act, practice or purpose.

**Disclosure** means the release of information to persons or organisations outside the Council. It

does not include giving individuals information about themselves.

**Eligible Data Breach** means when the unauthorised access, disclosure or loss of TFN information is likely to result in serious harm to one or more individuals.

**Freedom of Information Officer** means an individual employed by the Council who ensures compliance with the *Freedom of Information Act 1991*, who grants individuals the right to access information held by CoA. Freedom of Information Officers process requests for documents, assess whether information is exempt from disclosure and communicates decisions to applicants.

**Notifiable Data Breach Scheme (NDB)** means a scheme that the Council is subject to under the *Privacy Act 1988* to the extent that TFN information is involved in an Eligible Data Breach.

**Personal Information** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about a natural living individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, including a photograph or other pictorial representation of an individual, but does not include information that is in:

- generally available publications;
- material kept in public records and archives such as the Commonwealth or State archives; or
- anything kept in a library, art gallery or museum for the purpose of reference, study or exhibition.

**Sensitive Information** means information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association, a professional or trade association or a trade union;
- religious beliefs or affirmations;
- philosophical beliefs;
- sexual preferences or practices;
- criminal record; or
- health or biometric information.

**Voters Roll** means a list of entities that are enrolled and entitled to vote in a Council election.

## ADMIN

As part of Council's commitment to deliver the City of Adelaide Strategic Plan, services to the community and the provision of transparent information, all policy documents are reviewed as per legislative requirements or when there is no such provision a risk assessment approach is taken to guide the review timeframe.

This Policy document will be reviewed at least every four years unless legislative or operational change occurs beforehand. The next review is required in **August 2029.**

**Review history:**

| Trim Reference | Authorising Body | Date/ Decision ID | Description of Edits |
|---|---|---|---|
| | Council | XX Sep 2026 | Major Review |
| ACC2022/96413 | CEO | 29 July 2022 | Minor Review |
| ACC2021/130146 | CEO | 25th Oct 2021 | Minor review – added Privacy Impact Assessment Tool & Cookies |
| ACC2019/15874 | AD Information Management | 12th Feb 2019 | Minor review – added in Chatbot provisions and new template |
| ACC2008/52652 | Council | March 2016 | Major Review |

**Contact:**

For further information contact the Governance & Strategy Program
City of Adelaide
25 Pirie St, Adelaide, SA
GPO Box 2252 ADELAIDE SA 5001
+61 8 8203 7203
city@cityofadelaide.com.au