City of Hobart

Policy

Title: **Information Privacy**

CATEGORY: **Corporate Governance**

Date Last Adopted: 24 August 2020

1. Objectives

The policy statement sets out the Council's approach to managing, handling and protecting the personal information of customers and demonstrates its commitment to protecting the privacy of ratepayers.

2. Background

The City of Hobart collects and uses personal information about individuals to enable it to carry out its functions under the *Local Government Act 1993*. It also has the responsibility to keep information securely so as to protect the privacy of individuals, in accordance with the *Personal Information Protection Act 2004*, and relevant Federal legislation.

3. Policy

Purpose:

1. This policy statement sets out the Council's approach to managing, handling and protecting the personal information of customers.

2. The Council is committed to upholding the right to privacy of all individuals who have business dealings with the Council. The Council will take the necessary steps to ensure that the personal information that customers share with us remains confidential.

3. This policy will also serve to regulate and consolidate Council procedures in relation to the handling of personal information.

Scope:

1. This policy applies to employees and contractors of the Council.

2. The policy covers personal information that is collected, retained, stored and used by the Council where it is necessary for one or more of the Council's functions or activities.

3. Personal information is defined as:

   (i) Information or an opinion in any recorded format, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion and who is alive or has not been dead for more than 25 years.

   (ii) Examples of personal information held by the Council include; information relating to individual properties and property owners; the names of complainants and objectors; dog registration information; parking infringement information; rates information; and sensitive information such as health details collected on the DKHAC membership form.

Information Managers:

1. The Council has a number of information coordinators including the Manager Customer Services, Manager Human Resources, Manager Commercial Services and Rates, and the Manager Legal and Governance who oversee the operation of the Privacy Policy in consultation with the Council's legal team. Additionally there are trained Right to Information (RTI) officers included in all divisions. These staff will liaise with customers with respect to requests, enquiries and complaints regarding personal information kept by the Council.

2. The Council will receive customer requests for access to personal information and action these requests; respond to requests in writing; amend personal information; and liaise with the relevant divisions/units in relation to information requests and amendments. Staff will consult with the Council's Legal Team where appropriate.

The Collection of Personal Information:

1. It is the policy of the Council to collect personal information only if it is necessary for one or more of its functions or activities.

2. Certain information is collected in order to comply with laws and regulations.

3. Whenever the Council collects personal information, the information and the reasons for its collection will be shared with customers upon request. Requests of this nature are to be forwarded to the Council's Customer Services Manager.

4. The Council will only use personal information collected for the purposes for which it was collected and for any other use authorised or required by law, including law enforcement and compliance activities.

5. At the time that personal information is collected, or upon request, an individual will be provided with a copy of the Council's Privacy Statement. The Privacy Statement is a summary of the Privacy Policy and will be readily available and accessible to the public.

6. Sensitive information shall not be collected without express consent and unless the collection is required by law.

Use and Disclosure:

1. It is the Council's policy that personal information will not be divulged to third parties outside the Council for their independent use unless the person to which the information relates has authorised the Council to do so, or the disclosure is required or allowed by law. The Council and its employees will not sell, trade or make available personal information to others. Information provided by members of the public will only be shared with other business units within the Hobart City Council, where necessary.

2. Where the Council outsources functions that involve the collection, utilisation and/or holding of personal information, contractual measures shall be taken to ensure that the contractors and subcontractors do not act in a way that would amount to a breach of privacy standards. The Council will require that these vendors and service companies maintain the confidentiality of this information and abide by all applicable laws. This Council will not permit third parties to sell or use the information for their own purposes.

Data Quality:

The Council will take all reasonable steps to ensure that customers' personal information is accurate, complete and up-to-date. The Council will respond to any requests from the public to correct inaccurate information in a timely manner. Such requests must be forwarded to the Council's Customer Services Manager in the first instance.

Data Security:

1. The Council will take steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

2. Employees are responsible for protecting personal information from misuse, loss, corruption or disclosure. Personal information will be handled with care and only used for authorised purposes.

3. All employees must maintain public confidentiality and respect the privacy of individuals who have dealings with the Council. Employees must treat all personal information as confidential, and sensitive information as highly confidential. Council employees will not disclose any confidential information, use any information to their personal advantage or permit unauthorised access to information.

4. Requests for information from police, government agencies or anyone outside the Council, in regard to customers, should be directed to the Customer Services Manager and these will be referred elsewhere as required.

5. Council files are strictly confidential and under no circumstances should a member of the public have access to files. Employees must also be conscious of security within the office environment when members of the public are present. External customers must not be left unattended with Council files.

6. Where a complaint or objection is received by the Council the identity of the complainant shall not be disclosed.

7. The Council maintains security standards and procedures to help prevent access to confidential information by anyone not authorised to access such information. Employees are obliged to assist in maintaining security standards and procedures. Examples of the type of security measures that the Council has implemented and will continue to support include:

    (i) Physical security – the Council has adopted measures to prevent unauthorised entry to premises, systems to detect unauthorised access and secure containers for storing paper-based personal information;

    (ii) Computer and network security – the Council has adopted measures to protect computer systems and networks for storing, processing and transmitting personal information from unauthorised access, modification and disclosure;

    (iii) Communication security – Council has adopted measures to prevent unauthorised intrusion into computer networks; and

    (iv) Personnel security – the Council has adopted procedural and personnel measures for limiting access to personal information by authorised staff for approved purposes and controls to minimise security risks to the organisation's IT systems.

8. Destruction of records containing personal information, including personal records is by secure means. Ordinarily, garbage disposal or recycling of intact documents are not secure means of destruction and should only be used for documents that are already in the public domain.

(i) Reasonable steps to destroy paper documents that contain personal information include shredding, pulping or the disintegration of paper. All computers that are removed from use and made available for non-council purposes will have all data removed from the hardware.

Openness:

The Council has a Privacy Statement, which is a summary of this policy, readily available and accessible to the public. There is a link to the Privacy Statement on the internet and intranet. Hard copies of the Privacy Statement will always be available at the Customer Service Centre.

Access and Correction:

Individuals are entitled to access personal information about themselves which is held by the Council. Individuals are entitled to know generally what sort of personal information the Council holds about them, for what purposes, and how it collects, holds, uses and discloses that information.

1. Requests for access to such information are to be made in writing and forwarded to the Council's Customer Services Manager for action. Staff must establish the identity of the individual asking for the information.

2. If an individual has made a written request for access, the assigned officer will acknowledge the request as soon as possible or at least within 7 days of the request. If granting access is straight forward, it will be appropriate to grant access within 14 days, or if providing access is more complicated, within 30 days.

3. The Council will respond to public requests to correct information in a timely manner.

4. The Council will provide written reasons when a request for access or correction of personal information is refused

Anonymity:

Whenever it is lawful and practicable to do so, customers will be given the option of not identifying themselves when dealing with the Council.

Training:

All Council employees will receive training to increase their awareness in relation to the treatment of personal information in the workplace. Staff will be trained in security awareness, practices and procedures.

4. Legislation, Terminology and References

Section 130(3) of the Local Government Act 1993

Hobart City Council Privacy Statement

A Privacy Officer is a position within the Council that oversees the operational management and release of information under the Privacy Policy in consultation with the Council's legal team.

Personal Information for the purpose of this Policy is defined as:

> Information or an opinion in any recorded format, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion and who is alive or has not been dead for more than 25 years.

Sensitive information is defined as:

> Information or opinion about individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record, health information and financial status.

Types of security measures include, physical security, computer and network security, communication security and personnel security.

Responsible Officer:	Director City Enablers
Policy first adopted by the Council:	08/04/2002
History	
Amended by Council	17/12/2007
Amended by Council	12/09/2011
Amended by Council	07/03/2016
Amended by Council	23/09/2019
Approved by Council	24/08/2020
Next Review Date:	Within 2 years of last review.
File Reference:	F19/79648