

1. Purpose and Intent

Frankston City Council is committed to meeting community expectations regarding handling of personal information and its obligations under privacy legislation.

The *Privacy and Data Protection Act 2014* and the *Health Records Act 2001* require Council to document policies on its management of personal information and make the documents publicly available. This policy outlines Council's broad approach to minimising privacy risks and responding to privacy breaches and complaints. More detailed information about the handling and protection of personal information in specific contexts is available on Council's website.

2. Scope

This policy applies to all Council employees, contractors and volunteers undertaking duties on behalf of Council, and to Councillors.

The policy applies to the management of all personal, health and sensitive information handled by Council, including information about customers, residents, service providers, visitors and staff.

3. Definitions

Personal information: means information or an opinion that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion.

Health information: means information or an opinion about the physical, mental or psychological health of an individual; or a disability of an individual; or an individual's expressed wishes about the future provision of health services to him or her; or a health service provided to an individual; or other personal information collected to provide a health service.

Sensitive information: means information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, or criminal record.

Privacy breach: an act or practice that contravenes one or more of the Information Privacy Principles in the *Privacy and Data Protection Act 2014* or the Health Privacy Principles in the *Health Records Act 2001*, or the privacy principles in any another privacy law which applies to the specific type of personal information or type of service.

4. Authorisation

This policy is managed by the Governance and Information Department, and is approved by Frankston City Council's Mayor and Chief Executive Officer (CEO):



Mayor, Frankston City



CEO, Frankston City Council

in accordance with a resolution made by Frankston City Council at its meeting on 31/01/2022.

5. Policy

5.1 Privacy Principles

Council policies, procedures, services and strategies will be developed and delivered in accordance with the Information Privacy Principles in the *Privacy and Data Protection Act 2014*, the Health Privacy Principles in the *Health Records Act 2001* and other privacy laws which may apply to specific Council activities. Council will actively encourage privacy compliance and minimise privacy risk.

The Information Privacy Principles and Health Privacy Principles cover all aspects of collection, use, disclosure, management, security and retention of personal, health and sensitive information. In summary, Council's broad obligations are to:

- Allow people to interact with Council **anonymously**, where that is lawful and practicable.
- **Collect only the personal information that is necessary** for Council's functions.
- **Provide notice** about how the information will be used and disclosed.
- **Collect information directly from the person** where possible.
- **Use and disclose** personal information only for the primary purpose it was collected, a secondary related and expected purpose, as authorised by law, for certain emergency situations or with the person's consent.
- Take steps to make sure that personal information is **accurate, complete and up to date**.
- Take steps to **protect personal information** from misuse and loss and from unauthorised access, modification or disclosure.
- Provide processes for people to seek **access** to, or the correction of, their personal information.

The associated privacy impact will be assessed as part of decision making for new initiatives, processes, information systems and technology and steps taken to mitigate privacy risks as far as is lawful and practicable.

5.2 Privacy breaches and risks

All identified privacy breaches and privacy risks must be immediately reported to Council's Privacy Officer or, in the case of Councillors, to the Chief Executive Officer, who will assess the report and make decisions in relation to:

- the steps required to prevent the impact of a breach worsening
- whether notification to the affected people is appropriate
- whether notification to the relevant privacy regulator is required
- the steps to be taken to prevent similar future breaches or mitigate the identified privacy risk

5.3 Privacy complaints

Privacy complaints can relate to matters which are highly time sensitive and must be immediately referred to Council's Privacy Officer or the Chief Executive Officer.

All privacy complaints are investigated and the complainant is provided with information about the investigation and outcome. If a complainant is not satisfied with Council's response, they are entitled to refer their complaint to the Victorian Information Commissioner or Health Complaints Commissioner.

5.4 Privacy training

Council will actively encourage privacy awareness and compliance.

All Council staff will complete privacy awareness training during induction and regular privacy refresher training during their employment. Privacy awareness will be included in the Councillor induction program.

6. Roles and responsibilities

All staff, contractors, volunteers and Councillors are responsible for:

- ensuring that they are familiar with Council's privacy obligations and how they apply to their work
- applying the privacy principles to all handling of personal, health and sensitive information
- immediately reporting privacy breaches or identified privacy risks
- immediately referring privacy complaints

Executive Management Team (EMT) and all managers are responsible for:

- fostering a culture and values that enhance decision processes ensuring privacy is embedded in the work environment
- ensuring that the privacy impact associated with new initiatives is assessed and steps are taken to mitigate privacy risks

Privacy Officer is responsible for:

- providing clarification or advice about interpretation of the policy and the application of the privacy principles

- receiving, assessing and providing advice regarding the required response to notifications of privacy breaches and identified privacy risks
- receiving, assessing and responding to privacy complaints
- referring privacy matters involving potential staff misconduct to the Manager People and Culture

7. Policy non-compliance

Non-compliance with Council’s legislative privacy obligations and this policy has the potential to:

- cause harm to people impacted by a privacy breach
- cause reputational damage to Council
- hinder Council’s day to day operations if information systems are compromised
- generate complaints to the Victorian Information Commissioner or Victorian Health Complaints Commissioner
- constitute a breach of the provisions relating to confidential information in the *Local Government Act 2020*
- incur financial penalties for Council and/or individual Councillors and staff
- result in disciplinary action for staff

8. Related documents

Privacy and Data Protection Act 2014 (Vic)

Health Records Act 2001 (Vic)

Privacy Act 1988 (Fed)

Charter of Human Rights and Responsibilities Act 2006 (Vic)

Local Government Act 2020 (Vic)

Information Technology security policies and procedures

Records Management policy and associated guidance materials

9. Implementation of the Policy

This policy will be published on Council’s website and intranet. Managers, Coordinators and Team Leaders will be responsible for educating their staff about this policy, and for facilitating compliance. Governance and Information will provide guidance, support and training to assist compliance.

This policy will operate until it is revoked or varied by a Council resolution.

10. Document History

Date approved	Change Type	Version	Next Review Date