



PRIVACY MANAGEMENT FRAMEWORK

Version: 1

Published on 1st August 2020

Table of Contents

1. Glossary	2
2. Context	4
3. Purpose	4
4. Implementation	4
5. Guiding Principles	4
1. Transparency	4
2. Value.....	4
3. Collection Limitation	4
4. Safety First.....	4
5. Fair Decisions.....	4
6. Accountability.....	5
7. Agility.....	5
6. Expectations of Council.....	5
7. Privacy by Design – in activity	5
8. Privacy by Design – in leadership	5
Privacy Champion	6
Security Champion	6
9. Privacy Maturity	6
10. Privacy Management Plan.....	7
11. Smart City Privacy.....	7
12. Visual Representation.....	8
13. Review	8

Last updated:

Version: 1 | Amended: N/A | Last updated: 24.02.2020

1. Glossary

The PMF uses important key terms throughout:

Abbreviation or term	Expansion or definition
Contracted Service Provider (CSP)	The person or body that is collecting and handling personal information under a service contract with Council.
Best practice	In relation to privacy, best practices are globally accepted frameworks, guidelines, approaches or ideas that represent the most efficient or prudent course of action
Council	City of Darwin
Data	Information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic or digital form that can be stored and used by a computer or some other interface
Data breach	Unauthorised access to, disclosure or loss of personal information (as a security failure). Data breach is a relevant consideration for Council, including in relation to its industry-based Smart Darwin partners and contracted service providers.
Information Act	<i>Information Act 2002</i> (NT) which contains the Northern Territory's privacy principals, the IPPs
NT Privacy Commissioner	The Northern Territory Privacy Commissioner, who is Deputy Information Commissioner (Office of the Information Commissioner)
IoT	Internet of Things (and other connected) technologies
IPPs	The 10 Information Privacy Principles, as set out in the Information Act
PbD	Privacy by Design

Abbreviation or term	Expansion or definition
Personal information	<p>'Government information that discloses a person's identity or from which a person's identity is reasonably ascertainable', as defined in the Information Act.</p> <p>The understanding of personal information is broadened somewhat in the PMF (to the benefit of the community, and to align with privacy best practice) to include, as defined in the Privacy Act, 'information or an opinion about an identified individual or an individual who is reasonably identifiable'.</p>
PMF	Privacy Management Framework for Council. This is a strategic/ governance level document.
PMP	Privacy Management Plan for Council. This operationalises the PMF.
Privacy	Protection of personal information in accordance with the law
Privacy breach	An interference with privacy, as described in the Information Act. This is a failure to apply the IPPs, generally, in the collection and handling of personal information.
Privacy Champion	The nominated Council officer responsible for leading Council's management of statutory and best practice privacy requirements.
Privacy Policy	Council's Privacy Policy, which exists in the form of a community-facing Privacy Statement that explains how personal information is collected and handled. The Privacy Policy is a key document for ensuring community privacy awareness.
Record	Recorded information in any form (including data in a computer system) that is required to be kept by Council as evidence of its activities or operations. A record may include part of a record or a copy of a record.
Security	The physical, technical and administrative controls around that which must be protected (that being, personal information). Security represents only one of the multiple obligations set out in the IPPs in relation to the collection and handling of personal information. Security includes cybersecurity.
Security Champion	The nominated Council officer responsible for leading Council's management of its information security requirements, including statutory requirements, standards, frameworks and best practice.
Service contract	A contract or arrangement under which a person or body collects or handles personal information for or on behalf of Council
Smart Darwin	Council's smart city mandate, as described in the Smart Darwin Strategy
#SwitchingOnDarwin	The component of Smart Darwin to which a separate Privacy Framework refers

2. Context

In late-2019, the City of Darwin (Council) commenced a program of work dedicated to ‘privacy uplift’. In addition to enhancing Council’s capacity to meet or exceed the privacy and fair information handling requirements set out in the *Information Act 2002* (NT) (Information Act), the program of work supports embedding privacy considerations – and awareness generally – in all facets of Council business.

[Our Approach to Privacy](#) establishes at a strategic level what privacy means to Council and provides a foundation for Council’s Privacy Management Framework (PMF) (this document).

3. Purpose

Privacy is the protection of personal information in accordance with the law. It is additionally about meeting community expectations about the fair and transparent handling of personal information. The PMF supports privacy as a key consideration for Council and provides the structure for an ongoing program of privacy work.

In addition to responding to the privacy obligations set out in the *Information Act 2002* (NT), the PMF contains the supporting architecture to assist Council in achieving privacy ‘best practice’ in all aspects of business – both internal and community-facing – involving the collection and handling of personal information.

4. Implementation

The PMF will be implemented during the 2020 calendar year. During implementation, it is expected that appropriate levels of privacy advice will be sought to give effect to the Framework’s requirements (including independent privacy expertise, legal counsel and consultation with the NT Privacy Commissioner).

5. Guiding Principles

This PMF is **underpinned by** the seven guiding principles in [Our Approach to Privacy](#):

1. **Transparency** – Darwin is an aware and informed community.
2. **Value** – There is demonstrable value for the community in providing their personal information to Council.
3. **Collection Limitation** – Personal information is collected only when it is necessary for the performance of Council functions.
4. **Safety First** – Where personal information must be collected, it is securely stored and de-identified wherever possible before use or disclosure.
5. **Fair Decisions** – Lawful decisions about the collection and handling of personal information are made by Council, and the decisions reflect community values and expectations.

6. **Accountability** – Privacy by Design is supported for all initiatives involving personal information, privacy impact assessments are conducted, and Council’s privacy posture is regularly reviewed.
7. **Agility** – Council adapts and respond to changes in legislation, public policy, technology, the information economy and the emerging body of privacy best-practice.

6. Expectations of Council

The PMF **affirms** that Council is aware of, and committed to, meeting expectations that it will handle personal information lawfully and mindfully.

Council will observe its requirements under law, in particular that:

- Requirements set out in the Information Act and other relevant Territory and Federal laws are met; and
- Legislative and contractual requirements applicable to any contracted service providers are clear and adhered to.

Council will handle personal information in a manner that responds to community expectations, including that:

- Council’s program of privacy work is visible to the community;
- There is confidence in the community that privacy is a key consideration in all aspects of Council business involving personal information; and
- Privacy best practice is applied within Council as a matter of course.

7. Privacy by Design – in activity

The PMF **affirms** Council’s position that, in order to remain responsive to the seven guiding principles in [Our Approach to Privacy](#), a Privacy by Design (PbD) approach to decision-making, project design and other elements of Council business is crucial.

PbD is a best practice approach whereby privacy is *designed into* policies, procedures, processes, projects, initiatives, products, services and technologies – indeed, to all aspects of Council business involving personal information – as opposed to being *bolted on* later. It is about preventing privacy risk at the outset, rather than responding to risk after the fact – e.g., after complaint of privacy breach has been made or when Council is facing scrutiny of the NT Privacy Commissioner.

8. Privacy by Design – in leadership

PbD also reflects the desirability of achieving a strong privacy mindset (or culture) at all organisational levels, across all business functions, involving all staff, for all matters involving personal information and at all stages of the information lifecycle. Council considers that the responsibility for privacy compliance rests with the local government as a whole and that embedding a privacy mindset (comprised of cultural, risk management and legislative compliance elements) is vital.

The PMF **affirms** Council's position that, in order to give effect to PbD in its activities, Council must cultivate a culture that recognises and supports privacy as a leadership function.

To this end, the PMF confirms the support of the Chief Executive Officer for all strategic and operational privacy matters and **establishes** the following leadership roles:

- Privacy Champion
- Security Champion

Privacy Champion

The Privacy Champion is the nominated Council officer responsible for leading Council's management of statutory and best practice privacy requirements. The Privacy Champion is also Council's approved point of contact with the Office of the Information Commissioner in relation to matters involving privacy and protection of personal information in accordance with the Information Act.

Council's Privacy Champion is the **Executive Manager, Corporate Services**

Security Champion

A key component of strong privacy practice in Council is ongoing attention to information security requirements – particularly as regards taking reasonable steps to ensure personal information is secure throughout its lifecycle.

The Security Champion is the nominated Council officer responsible for leading Council's management of its information security requirements, including statutory requirements, standards, frameworks and best practice. Together with the Privacy Champion, the Security Champion ensures that Council applies reasonable administrative, technical and physical safeguards in its management of personal information.

Council's Security Champion is the **Executive Manager, Innovation and Information Services**

It is noted that, at present, the roles of the Privacy Champion and Security Champion have both been "self-nominated" as part of Council's privacy uplift process. The roles are not remunerated but are, rather, considered complementary to the existing leadership positions of the relevant officers.

By or before the June 2021 review of the PMF, Council will consider whether these important roles require additional support.

9. Privacy Maturity

Council must be able to measure and report on the extent of its privacy program and improvements made over time. The PMF **establishes** the tracking of Council's privacy program maturity using a purpose-built Maturity Model.¹

¹This is an internal operational document of Council, however the metrics have been designed to allow Council to score and report on progress.

The Maturity Model reflects matters of strategic and operational necessity for a successful privacy program and offers Council ongoing opportunities to improve. The Maturity Model establishes key metrics across the following areas:

1. Governance and Culture;
2. Privacy Strategy;
3. Privacy Processes;
4. Risk and Assurance; and
5. Data Breach Response.

The Maturity Model is designed to:

- Encourage growth and excellence of privacy practice over time;
- Form the basis of Council's Privacy Management Plan; and
- Provide Council with a way to measure and report on its success.

10. Privacy Management Plan

Through its establishment of a Maturity Model, the PMF **directly supports** Council's Privacy Management Plan (PMP). Likewise, the PMP operationalises the objectives of the PMF.

The PMP is an internal operational document of Council that has a 2-year review cycle. The PMP reflects action items relevant to Council as a whole, whereby completion of each action item strengthens and elevates Council's privacy posture – whether via policies, procedures or processes, or via awareness initiatives, or via strengthening ancillary activities in Council (such as information security and risk management).

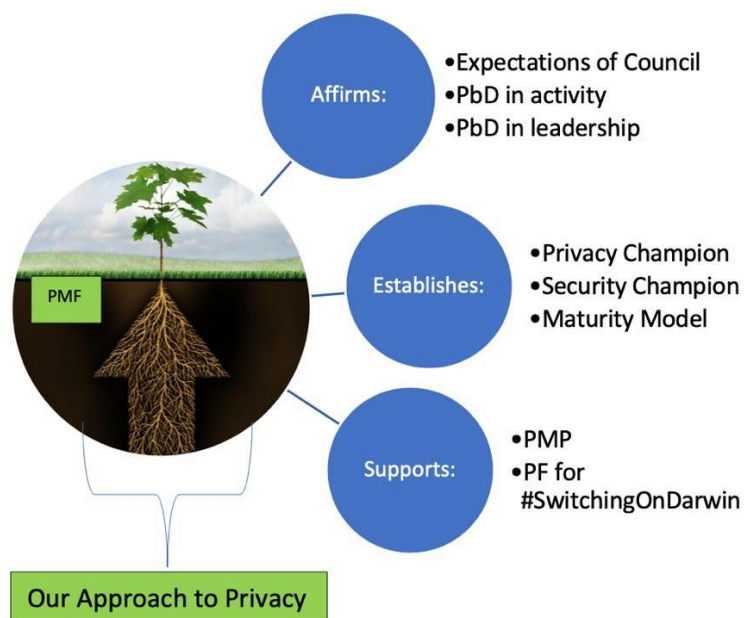
Strong operational attention to the PMP reflects Council's PbD considerations, as well as statutory obligations and community expectations.

11. Smart City Privacy

A 'smart city' leverages technology (e.g. IoT and connected technologies) and urban data, which may include personal information of members of the community, for beneficial public purposes. Through its Smart Darwin strategy, which includes the technologies supported by the #SwitchingOnDarwin program, Council continues to increase its smart city capacity.

Council has in place a specific [Privacy Framework for #SwitchingOnDarwin](#). That framework is **supported** by the PMF and is cross-referenced within Council's PMP.

12. Visual Representation



13. Review

The PMF will be reviewed in June 2021 to ensure ongoing alignment with [Our Approach to Privacy](#).

Any amendments to the PMF will be clearly referenced in version control, using version number and date, as follows:

Version: 1 | Amended: n/a | Last updated: 24/02/2020

