#SwitchingOnDarwin – Privacy Framework

Table of Contents

Context:

Smart Cities

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.

Australian local governments pursing smart city goals must consider the legal environment they operate in (including federal and state/ territory laws that apply to them), best practice imperatives and community expectations as part of their process. Information security and privacy requirements will inform how a city collects, uses and manages personal information and the extent of any privacy risks (whether real or perceived).

To attain smart city goals, a city must find a balance between promoting information availability (on the one hand) and ensuring privacy of those in the community (on the other). Transparency about the extent to which personal information is involved in smart city initiatives, including how such information will be managed, is key to maintaining community trust.

Smart Darwin

The City of Darwin (Council) recently received a total of $10 Million in funding for its own smart city initiative, #SwitchingOnDarwin, from Federal, Territory and Local Government sources. The funding enabled the purchase of six technologies and the establishment of digital infrastructure to underpin Council's Smart Darwin Strategy (Smart Darwin). This represents the largest single smart city initiative in Australia.

Smart Darwin involves using technology to enhance the community experience of visiting, living and working in the City of Darwin, and the making of aggregate and statistical data:

- available to the public via dedicated disclosure portals (ArcGIS and OpenGov);
- able to be combined and analysed in the context of community-based data insights (Neighbourlytics and Readify); and
- accessible through a 'community data exchange' environment that serves the information needs of citizens, public policy makers, innovation hubs, tourism and other industries.

#SwitchingOnDarwin

#SwitchingOnDarwin is about the commissioning of the following six technologies and the digital infrastructure that underpins them. The six technologies are:

- Smart CCTV
- Public Wi-Fi
- Environmental Sensors
- Smart Parking
- Wayfinding
- Smart Lighting

#SwitchingOnDarwin is underpinned by the following public policy goals:

- Enable better decision making by using technology and data to support decisions;
- Have more real time data, rather than delayed information (meaning Council can quickly respond to needs);

- Provide the community with a safer city and reduce antisocial behaviour;
- Use technology to help save energy;
- Provide more convenient services to the community; and
- Find efficiencies in how Council operates to minimise costs.

Privacy for #SwitchingOnDarwin

In response to community expectations and concerns about some of the #SwitchingOnDarwin technologies, in particular the Smart CCTV technology, Council has committed to establishing a Privacy Framework (Framework). The Framework is consistent with Council's Privacy Policy and is part of the ongoing body of privacy work detailed in Our Approach to Privacy.

Privacy Framework:

Last updated:

Version: 1 | Amended: N/A | Last updated: 20.09.2019

1. Glossary

This Framework uses important key terms throughout:

Abbreviation or term	Expansion or definition
Aggregate	De-identified information assembled in a class, cluster or cohort of sufficient size
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
Contracted Service Provider (CSP)	The person or body that is collecting and handling personal information under a service contract with Council. The Council refers to some #SwitchingOnDarwin CSPs as 'technology partners' in existing documentation
Council	City of Darwin
CCTV	Closed Circuit Television
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

Abbreviation or term	Expansion or definition
Data breach	Unauthorised access to, disclosure or loss of personal information (as a security failure). Data breach is commonly understood in the context of NDBR, however is a relevant consideration for Council and its industry-based Smart Darwin partners.
De-identify	Remove identifying particulars so as to render personal information 'not identifiable'
FR	Facial recognition technology
Information Act	*Information Act 2002* (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
NDBR	Notifiable Data Breach Reporting, as required under the Privacy Act
OAIC	Office of the Australian Information Commissioner
PbD	Privacy by Design
Personal information	'Government information that discloses a person's identity or from which a person's identity is reasonably ascertainable', as defined in the Information Act. The understanding of personal information is broadened somewhat in this Framework (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'.
PIA	Privacy Impact Assessment
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 Act	*Privacy Act 1988*
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 Policy	Council's Privacy Policy, which explains for the community how personal information is collected and handled. The Privacy Policy is a key

Abbreviation or term	Expansion or definition
	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.
Sanitisation	De-identification of personal information for use in system testing, data analysis and publishing
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.
Sensitive information	A subset of personal information, as defined in the Information Act, where the personal information is health information or is about: • racial or ethnic origin; or • political opinions; or • membership of a political association; or • religious beliefs or affiliations; or • philosophical beliefs; or • membership of a professional or trade association; or • membership of a trade union; or • sexual preferences or practices; or • a criminal record.
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 this Framework refers

2. Purpose

This Framework sets the **expectations** and **decision-making criteria** for how #SwitchingOnDarwin technologies are deployed and used and the way data (in particular, personal information) is collected and managed.

In addition to responding to the privacy obligations set out in the *Information Act 2002* (NT), this Framework is concerned with ensuring Council achieves privacy 'best practice' and actively meets community expectations around privacy and the protection of personal information.

The Framework will be implemented during the commissioning of #SwitchingOnDarwin technologies. 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).

The Framework will be reviewed post-implementation to ensure ongoing alignment with Council's Approach to Privacy.

Important: Application of the Framework is specific to #SwitchingOnDarwin and does not remove Council's obligation to consider privacy in the context of how it governs IoT deployments for Smart Darwin going forward. This Framework, its implementation and Council's program of privacy work, generally, should inform the drafting of Council's Smart Darwin IoT Governance Framework and related documentation.

3. Guiding Principles

This Framework corresponds with 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.

4. The Tech

In addition to the underpinning digital infrastructure, #SwitchingOnDarwin includes the following technologies:

- Smart CCTV

- Public Wi-Fi
- Environmental Sensors
- Smart Parking
- Wayfinding
- Smart Lighting

A brief summary of the technologies is below:

Smart CCTV

Smart CCTV cameras have provided Council with an opportunity to gather insight into how the community uses their urban spaces, footpaths, roads and public venues. This insight is considered both valuable and aligned with the smart city ethos of using data for good (that is, to benefit the public).

The Smart Darwin strategy additionally notes the importance of a safe city:

> *"Public safety and crime prevention are important to the Darwin community and a high priority of council and the government. The addition of more CCTV cameras in strategic locations across the city allow for both prevention and solving of crime."*[1]

The Smart CCTV cameras offer Facial Recognition (FR) as a capability; however, Council has made a public commitment not to activate or use FR. This commitment is of critical importance to the community.

Public Wi-Fi

#SwitchingOnDarwin expands Council's existing free Wi-Fi network. It is a draw-card for the community and visitors alike to enjoy Darwin's public spaces, experience convenience when visiting local businesses and work remotely without interrupted internet access.

In addition, and importantly, Council has the opportunity to assess the value of free Wi-Fi for the community and local businesses – for example, does being 'connected' entice people to stay longer in a café, relax with friends in the park or attend events in the vicinity?

Environmental Sensors

Microclimate sensors and other sensing devices collect a range of data about Darwin's environment such as rainfall, humidity, air quality and CO2 levels. The data can be analysed to develop specific insights about the impact of environment on Darwin's quality of life and sustainability, and those insights can be used by Council, local business, government and others to inform decision making.

[1] https://www.darwin.nt.gov.au/council/transforming-darwin/smart-darwin/making-our-city-smarter

For Council, the ability to add cooling and greening initiatives to public spaces and improve real-time weather warnings are important priorities.

Smart Parking

Smart Parking involves helping drivers to locate available parking by seeing a visual indicator or by using an app. If using an app, drivers also have the opportunity to pay for their parking without going to the kerbside payment kiosk.

The Smart Darwin strategy explains the benefits of implementing Smart Parking:

> *"Traffic congestion should ease, and vehicle emissions should decrease as a result of being able to locate a parking spot with greater convenience.*
>
> *Additionally, the ability to pay for parking and for council to monitor parking more efficiently and understand parking usage and demand at any given time, are added benefits."*[2]

Wayfinding

The Smart Darwin strategy characterises the Wayfinding component of #SwitchingOnDarwin as:

> *"Community facing digital stations that will provide information and enable interaction with council."*[3]

Council has installed a number of Wayfinding kiosks which operate as interactive maps. The kiosks "push" information to people who access them; for example, points of interest along a walking route.

Smart Lighting

The replacement of Council street lights with LED Smart Lighting creates the potential for lighting levels to be adjusted to brighten an area for an event or other activity or, at the request of Police, to help deter crime and anti-social behaviour. The lights are able to sense changes to light levels and automatically adjust; for example, in response to the darkening caused by an incoming storm.

In addition, motion sensors within the Smart Lighting can help Council determine how often and at what times of day public spaces are being used.

Click here to see an interactive map of the #SwitchingOnDarwin technologies. For now, the technologies will be used in the city centre only.

[2] Ibid
[3] Ibid

5. Expectations

From a privacy perspective, any collection and handling of personal information for any Council initiative must be done in accordance with the law. Additionally, community privacy expectations are important for Council to understand and act on.

For #SwitchingOnDarwin, it is expected that (at a minimum)--

Law

- Requirements set out in the *Information Act 2002* (NT) and other relevant Territory and Federal laws are met; and
- Legislative and contractual requirements applicable to any Contracted Services Providers are clear and adhered to.

Community expectations

- #SwitchingOnDarwin data is used for good; that is, for the benefit of the community;
- The community understands the value in sharing their personal information with Council;
- Concerns raised by the community about any of the #SwitchingOnDarwin technologies are taken seriously; and
- Privacy best practice is applied to the greatest extent possible.

6. Decision-Making Criteria and Key Actions

The below decision-making criteria (Criteria) and key actions (A) are summarised for ease of reference at Appendix A.

6.1. [CE] Community engagement

Ensuring a strong trust relationship with the community is vital. Where there are concerns about #SwitchingOnDarwin technologies, there should be a mechanism for those concerns to be heard. The mechanism should exist separately from Council's privacy complaints process and be considerate of culture, languages, age groups, disabilities and other factors that may impact the community's ability to raise their concerns.

[CE] Criteria 1: The community is able to engage with Council about privacy concerns relating to #SwitchingOnDarwin technologies.

A1: Council will provide opportunities to engage with the community, and accept community feedback, about privacy concerns relating to #SwitchingOnDarwin technologies.

6.2. [PbD] Privacy by design – building privacy in from the outset

The foundational concept of Privacy by Design (PbD) is that privacy and protection of personal information are built directly into technology, systems and practices at the design phase. PbD is about ensuring a strong privacy mindset (or culture) where preventing privacy risk at the outset is a key focus.

While the #SwitchingOnDarwin initiative is already underway, and while the technologies have already been purchased, the use of Privacy Impact Assessment (PIA)s to pinpoint and address privacy risks is a critical opportunity for Council to explore.

Understanding *what data is involved* (e.g. data elements, including any personal information) and *how the data flows* (e.g. how it is collected, where it is stored, when and how it is sanitised, and where it ends up) are key components of any PIA.

[PbD] Criteria 1: Privacy is embedded throughout the remaining lifecycle of the #SwitchingOnDarwin initiative, with a focus on considering privacy risk in a proactive and preventive way.

A1: To ensure PbD informs the commissioning of #SwitchingOnDarwin technologies, Council will implement this Framework.

[PbD] Criteria 2: Privacy Impact Assessment (PIA)s are conducted at the outset of an initiative (and at key junctures thereafter) to pinpoint and address privacy risk.

A1: PIAs will be conducted for all #SwitchingOnDarwin technologies that involve personal information.

A2: There will be an accurate accounting of the data elements associated with #SwitchingOnDarwin, including any personal information therein.

A3: Data flows will be documented to identify potential points of risk to personal information.

6.3. [APL] Application of privacy law

Council is required to comply with requirements set out in the laws of NT and Australia; significantly, the privacy requirements set out in the Information Act.

[APL] Criteria 1: The privacy requirements set out in applicable laws of the NT and Australia are met.

A1: Council will apply privacy controls in accordance with the IPPs of the Information Act.

A2: Council will additionally address the action items listed in [PC] Privacy controls.[4]

A3: Council is to consider, as part of implementation of this Framework, the appropriateness of entering into a Code of Practice for #SwitchingOnDarwin in the manner set out in Division 3 of the Information Act.

6.4. [PC] Privacy controls

The below privacy controls are relevant as complementary, or in addition, to those set out in the IPPs of the Information Act.

6.4.1. [T] Transparency – *"Help me understand #SwitchingOnDarwin"*

Transparency is about making things visible for the community, such as how Council conducts its business, what initiatives are underway and the outcomes the community can expect. In privacy law, transparency also relates to making personal information handling practices visible for the community.

[PC: T] **Criteria 1:** The community understands the purposes for which their personal information may be collected by #SwitchingOnDarwin technologies.

A1: The purposes for which personal information is collected for #SwitchingOnDarwin are explained in Council's public-facing Privacy Policy and other publications.

6.4.2. [N] Notice – *"Tell me when my personal information is being collected"*

An important feature of privacy is the giving of notice. Notice means that, when personal information is collected (or as soon as possible afterward), the community is told what personal information is being collected, why it is being collected and what will happen to it.

Notice is given to provide an explanation of the personal information Council needs in order to conduct its business. ***Notice is not the same as consent***. Consent is where the Council asks permission to collect personal information (e.g. where the information is 'sensitive information').

[PC: N] **Criteria 1:** The community is notified when their personal information is being collected by #SwitchingOnDarwin technologies.

[4] Where there is inconsistency with the IPPs of the Information Act, the action that meets the higher privacy threshold will apply.

A1: Council will provide adequate signage and other forms of notice to inform the community that they are entering/ in an area where #SwitchingOnDarwin technologies are in operation.

A2: Council will determine whether consent is required for the collection of personal information by any of the #SwitchingOnDarwin technologies.

6.4.3. [CL] Collection limitation – *"Only collect the personal information you need from me"*

Although there is value in having a lot of data to work with in a smart city, privacy law requires that Council collects only the personal information it needs. This means that collection of personal information by #SwitchingOnDarwin technologies must be limited and specific.

[PC: CL] **Criteria 1:** Collection of personal information to be limited to that which is necessary to fulfil the functions of the #SwitchingOnDarwin technologies.

A1: Council will identify what personal information, if any, is necessary to collect via each #SwitchingOnDarwin technology. Only the necessary personal information will be collected.

6.4.4. [UL] Use limitation – *"Limit how my personal information will be used"*

When personal information is collected for one purpose, it is imperative that it is only used for that purpose (unless a valid exception or exemption set out in the Information Act can be applied). This ensures ongoing compliance with privacy requirements and, importantly, is consistent with community expectations.

[PC: UL] **Criteria 1:** To avoid doubt, the purpose for which personal information is collected via #SwitchingOnDarwin technologies is made clear at the outset (e.g. through Notice). The personal information is then only used for that purpose.

A1: Council will limit ancillary uses of personal information collected through #SwitchingOnDarwin technologies by ensuring the purpose of collection is made clear through Notice and other forms of communication.

6.4.5. [AFC] Avoid function creep – *"Maintain my expectation of privacy"*

'Function creep' is the gradual widening of the use of a technology to include purposes the technology was not originally intended for (e.g. using mobile phone tracking in shopping malls to find out user shopping preferences). The combination of technologies can also signal function creep. In some cases, this can be considered innovative or efficient (which

would be seen to accord with smart city goals), however care must be taken to limit privacy impacts.

[PC: AFC] **Criteria 1:** Limit function creep associated with #SwitchingOnDarwin technologies.

A1: Where it is proposed use a #SwitchingOnDarwin technology for a new purpose, or to combine a #SwitchingOnDarwin technology with other technologies, a PIA will be conducted.

6.4.6. [IS] Information security – *"Keep my personal information safe"*

Security can be seen as the fence around that which Council must protect (e.g. personal information). Where IoT and other connected technologies are involved, security must be able to address the challenges of managing data in a digital environment.

For initiatives like #SwitchingOnDarwin, a strong information security posture ensures that personal information is kept safe throughout its lifecycle. To ensure compliance with the Information Act, the location(s) where personal information is stored will be important to consider.

[PC: IS] **Criteria 1:** Physical, technical and administrative controls are used to ensure the security of any personal information collected via #SwitchingOnDarwin technologies.

A1: Personal information collected by #SwitchingOnDarwin technologies will be held securely in Council's dedicated internal data management environments or in verified secure CSP environments.

A2: Where a CSP is involved with the collection and management of personal information for a #SwitchingOnDarwin technology, security requirements will be clearly set out per [PC: CSP-M] Criteria 1.

A3: Information security policies and procedures will reflect the unique risks posed by digital (and connected) technologies and environments.

6.4.7. [D-ID] De-identification of personal information – *"Maintain my trust"*

The publication of personal information, intentionally or otherwise, in publicly available data sets associated with Smart Darwin would generally be outside the expectations of the community. Where it is desirable to publish data to public platforms, and particularly where data sets are likely to be combined, analysed and manipulated to reveal insights or trends in relation to community interactions with the city, personal information must first be removed.

Privacy regulator guidance about de-identification is highly relevant, as a failure to properly de-identify personal information can lead to data breach and other unintended consequences. When used effectively, de-identification can help build trust in data governance processes overall.

[PC: D-ID] **Criteria 1:** Personal information collected via #SwitchingOnDarwin technologies is not included in publicly available data sets.

A1: Where personal information is part of a data set intended to be made available via Smart Darwin initiatives (e.g. the 'community data exchange'), it will be robustly de-identified first. If it cannot be de-identified sufficiently, it will not be used.

6.4.8. [MR] Managing Risks – *"Tell me about risks to my privacy and how they are dealt with"*

As highlighted in [PbD] Criteria 2, the assessment and ongoing management of privacy risk is an important part of Council's privacy program. PIAs also present an opportunity to share information about initiatives with the community; in many cases, helping to allay fears and concerns.

[PC: MR] **Criteria 1:** Privacy risks and management strategies for #SwitchingOnDarwin technologies are understood by the community.

A1: PIAs for #SwitchingOnDarwin technologies will be published in an easy to access location on Council's website.

[PC: MR] **Criteria 2:** PIAs are not treated as 'set and forget' documents; rather, they are adopted as an ongoing risk identification and management approach.

A1: PIAs completed for each #SwitchingOnDarwin technology will be reviewed on a scheduled basis and, if necessary, repeated.

6.4.9. [P-CCTV] Information sharing with Police – CCTV footage – *"Show me that Council will keep its promise"*

There is a historical relationship with Council and NT Police in relation to the purchase and deployment of CCTV cameras in the city centre. From a privacy perspective, it is imperative to ensure clarity around the treatment of CCTV footage collected using Council-owned cameras.

Council has made a strong public commitment that it will not use the facial recognition capability included in the Smart CCTV cameras acquired for #SwitchingOnDarwin.

[PC: P-CCTV] **Criteria 1:** Arrangements in relation to the management of the Smart CCTV camera system – including responsibility for maintaining the assets (cameras), network(s) used, manner of collection and use of CCTV footage, and data security – are formalised.

A1: Council will formalise the terms of its CCTV arrangements with NT Police in a Memorandum of Understanding (MOU).

A2: The MOU will affirm Council's strict position that CCTV footage collected via Council Smart CCTV cameras will not be subjected to facial recognition analysis.

[PC: P-CCTV] **Criteria 2:** Consultation with the NT Privacy Commissioner is initiated with respect to ongoing compliance with the Information Act.

A1: Council is to explore with NT Police and the NT Privacy Commissioner the appropriateness of entering into a Code of Practice, in the manner set out in Division 3 of the Information Act, for the collection and use of CCTV footage.

6.4.10.[CSP-M] Contracted Service Provider management – *"Control how others handle my personal information"*

The privacy landscape in Australia and globally is complex. Industry-based vendors, service suppliers and platforms are unlikely to be captured by the same privacy law as Council, however they play a critical role in ensuring that Council's privacy obligations are upheld.

Where Contracted Service Provider (CSP)s are required to comply with the federal *Privacy Act 1988*, there are mandatory data breach reporting requirements they must consider under the Notifiable Data Breach Reporting (NDBR) scheme. It is vital that all contracts in relation to #SwitchingOnDarwin clearly express the privacy, data security and NDBR obligations of CSPs.

Even where data breach reporting is not mandatory for a CSP, the identification and management of data breaches should be viewed as a critical component of any Council contracts with CSPs.

[PC: CSP-M] **Criteria 1:** Contracted Service Provider (CSP)s involved with supplying, commissioning and maintaining #SwitchingOnDarwin technologies and the underpinning digital infrastructure understand and uphold their obligations with respect to privacy and the protection of personal information.

A1: Council will review all contracts with CSPs to ensure that appropriate clauses relating to privacy, data security and management of suspected or actual data breach events have been included.

7. Complementary City policies

The implementation of this Framework will necessarily involve consideration of complementary existing Council policies and processes, such as those in relation to information security and risk management.

8. Oversight – *"Who is watching over my privacy?"*

Council has initiated and will continue consultation with the NT Privacy Commissioner about privacy considerations for #SwitchingOnDarwin.

9. Review – *"Will this Framework change?"*

Agility and adaptability are key to ensuring personal information is protected throughout its lifecycle. If gaps in privacy controls are identified during, or following, implementation of this Framework, the Framework will be amended to address the gap.

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

Version: 1.1 | Amended: Links included | Last updated: 21.02.2020

Appendix A – Summarised criteria and actions

Key criteria

	CE	PbD	APL	PC → *Complementary privacy controls*
C1	The community is able to engage with Council about privacy concerns relating to #SwitchingOnDarwin (SOD) technologies.	Privacy is embedded throughout the remaining lifecycle of the #SOD initiative, with a focus on considering privacy risk in a proactive and preventive way.	The privacy requirements set out in applicable laws of the NT and Australia are met.	
Action	A1: Council will provide opportunities to engage with the community, and accept community feedback, about privacy concerns relating to #SOD technologies.	A1: To ensure PbD informs the commissioning of #SOD technologies, Council will implement this Framework.	A1: Council will apply privacy controls in accordance with the IPPs of the Information Act. A2: Council will additionally address the action items listed in [PC] Privacy controls. A3: Council is to consider, as part of implementation of this Framework, the appropriateness of entering into a Code of Practice for #SOD in the manner set out in Division 3 of the Information Act	
C2		Privacy Impact Assessment (PIA)s are conducted at the outset of an initiative (and at key junctures thereafter) to pinpoint and address privacy risk.		
Action		A1: PIAs will be conducted for all #SOD technologies that involve personal information. A2: There will be an accurate accounting of the data elements associated with #SOD, including any personal information therein. A3: Data flows will be documented to identify potential points of risk to personal information.		

Complementary privacy controls

→	T	N	CL	UL	AFC	IS	D-ID	MR	P-CCTV	CSP-M
C1	The community understands the purposes for which their personal information may be collected by #SOD technologies.	The community is notified when their personal information is being collected by #SOD technologies.	Collection of personal information to be limited to that which is necessary to fulfil the functions of the #SOD technologies.	To avoid doubt, the purpose for which personal information is collected via #SOD technologies is made clear at the outset (e.g. through Notice). The personal information is then only used for that purpose.	Limit function creep associated with #SOD technologies.	Physical, technical and administrative controls are used to ensure the security of any personal information collected via #SOD technologies.	Personal information collected via #SOD technologies is not included in publicly available data sets.	Privacy risks and management strategies for #SOD technologies are understood by the community.	Arrangements in relation to the management of the Smart CCTV camera system – including responsibility for maintaining the assets (cameras), network(s) used, manner of collection and use of CCTV footage, and data security – are formalised.	Contracted Service Provider (CSP)s involved with supplying, commissioning and maintaining #SOD technologies and the underpinning digital infrastructure understand and uphold their obligations with respect to privacy and the protection of personal information
Action	A1: The purposes for which personal information is collected for #SOD are explained in Council's public-facing Privacy Policy and other publications.	A1: Council will provide adequate signage and other forms of notice to inform the community that they are entering/ in an area where #SOD technologies are in operation A2: Council will determine whether consent is required for the collection of personal information by any of the #SOD technologies	A1: Council will identify what personal information, if any, is necessary to collect via each #SOD technology. Only the necessary personal information will be collected.	A1: Council will limit ancillary uses of personal information collected through #SOD technologies by ensuring the purpose of collection is made clear through Notice and other forms of communication.	A1: Where it is proposed use a #SOD technology for a new purpose, or to combine a #SwitchingOnDarwin technology with other technologies, a PIA will be conducted.	A1: Personal information collected by #SwitchingOnDarwin technologies will be held securely in Council's dedicated internal data management environments or in verified secure CSP environments. A2: Where a CSP is involved with the collection and management of personal information for a #SOD technology, security	A1: Where personal information is part of a data set intended to be made available via Smart Darwin initiatives (e.g. the 'community data exchange'), it will be robustly de-identified first. If it cannot be de-identified sufficiently, it will not be used.	A1: PIAs for #SOD technologies will be published in an easy to access location on Council's website.	A1: Council will formalise the terms of its CCTV arrangements with NT Police in a Memorandum of Understanding (MOU). A2: The MOU will affirm Council's strict position that CCTV footage collected via Council Smart CCTV cameras will not be subjected to facial recognition analysis.	A1: Council will review all contracts with CSPs to ensure that appropriate clauses relating to privacy, data security and management of suspected or actual data breach events have been included.

→	T	N	CL	UL	AFC	IS	D-ID	MR	P-CCTV	CSP-M
						requirements will be clearly set out per [PC: CSP-M] Criteria 1. A3: Information security policies and procedures will reflect the unique risks posed by digital (and connected) technologies and environments.				
C2								PIAs are not treated as 'set and forget' documents; rather, they are adopted as an ongoing risk identification and management approach.	Consultation with the NT Privacy Commissioner is initiated with respect to ongoing compliance with the Information Act.	
Action								A1: PIAs completed for each #SOD technology will be reviewed on a scheduled basis and, if necessary, repeated.	A1: Council is to explore with NT Police and the NT Privacy Commissioner the appropriateness of entering into a Code of Practice, in the manner set out in Division 3 of the Information Act, for the collection and use of CCTV footage.	