NSW Smart Places Data Protection Policy

Document number:	Version number: 1
Date: November 2021	

Contact details

Business Unit: NSW Data Analytics Centre (DAC)	Division: Customer, Delivery & Transformation (CDT)
Email: datansw@customerservice.nsw.gov.au	

July 2022

Table of Contents

1. Policy Overview

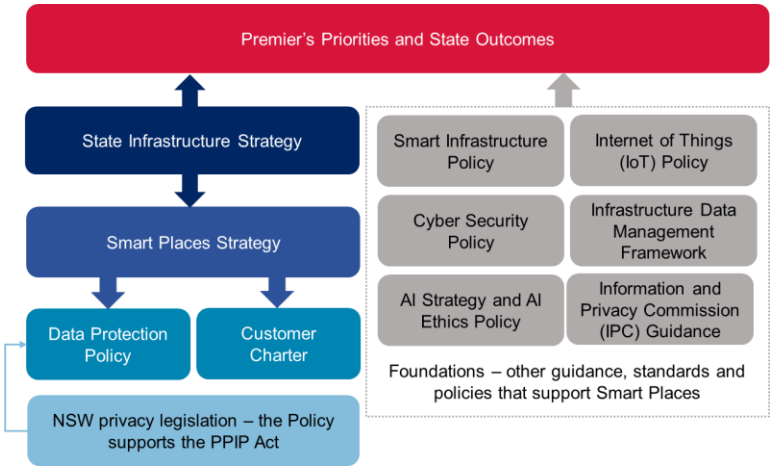
1.1 Introduction

The NSW Smart Places Strategy was launched in August 2020 to support NSW Government, local councils and private industry partners to harness the power of digital technologies and successfully bring 'smart' solutions to life in the cities, towns and communities of NSW.

The development of a Data Protection Policy (this document) is identified as an action in the Smart Places Strategy. This Policy brings key guidance on data protection in the smart places context together in one place. It aligns with the NSW Government Data Strategy which includes the central theme of strengthening transparency and trust in the way NSW government collects, manages, uses and shares data, ensuring this is in accordance with the highest privacy, security and ethical standards.

Smart places integrate sensors and other technology into the built and natural environments to capture, store, and make available data and insights, which are used to make decisions on improving productivity, liveability and resilience of cities, towns and communities. This includes anything from adjusting lighting in public parks based on the time of day to generating insights about the best way to respond to a disaster situation.

The Smart Places Strategy sets out foundations for implementing smart places, including standards and policies. These include the IoT Policy, Smart Infrastructure Policy, Cyber Security Policy and the AI Strategy and associated AI Ethics Policy. Smart places are necessarily data driven and these foundational policies provide guidance on privacy, security, and ethical considerations when using sensors and other technology to generate data and use it for decision-making. In addition, the Infrastructure Data Management Framework supports the use of data for the design, development and operation and maintenance of the built environment and the NSW Information and Privacy Commission has issued guidance on assessing information access and privacy impacts for projects seeking funding from the Digital Restart Fund, including for smart places.



1.2 Who is this policy for?

This Policy applies to all NSW Government agencies. It is designed to provide users with information needed to build data protection into smart places project design, and actively manage smart places data from collection to disposal. It provides guidance to help organisations follow lawful and best practice protection of smart places data.

This Policy supports the NSW Smart Places Customer Charter, in particular Principle 4 Keeping Customer Information Safe. Government agencies involved in smart places initiatives will adhere to the Policy. It is recommended that other place owners and smart places practitioners aspire to a similar level of best practice.

Other users of this policy may include members of the public, local councils, private industry contractors and those who collect, access, hold or process data obtained from a NSW Smart Place, as part of their commitments under the Customer Charter.

1.3 The purpose of the policy

The purpose of the Data Protection Policy as stated in the Smart Places Strategy, is to support the *Privacy and Personal Information Protection Act 1998* (PPIP Act), to guide how data is collected, managed and stored as part of smart places implementation.

The PPIP Act outlines how NSW public sector agencies manage personal information. Personal information is defined in section 4 of the PPIP Act as “Information or an opinion (including information or an opinion forming part of a database and whether or not in recorded form) about an individual whose identity is apparent of can be reasonably ascertained from the information or opinion”. In practical terms, personal information could include written records with a person’s name and address, photographs, video or audio footage of individuals, or a person’s fingerprints, blood or DNA. Personal information can also include information that is observed, generated or inferred about a person, even incidentally, from smart places technology. The Information Protection Principles (IPPs) are part of the PPIP Act and define the obligations that NSW public sector agencies, statutory authorities, universities and local councils must put into practice when they collect, store, use or disclose personal information.

The *Health Records and Information Privacy Act 2002* (HRIP Act) identifies Health Privacy Principles (HPPs) and specifies similar obligations to protect health information. HRIPA applies to public sector agencies, private sector organisations that provide a health service or collect, hold or use health information and private sector organisations including some businesses that are related to another business, with an annual turnover of more than $3 million that collect, store and use health information.

This Policy does not impact on an individual’s legislative rights regarding data and personal information which NSW Government is bound to adhere to, and nor does it prevent or limit existing law.

Because smart places and the technology are so diverse, providing advice suitable for every smart places project is impractical. Rather, this policy provides practical guidance and advice for smart places practitioners who are planning, creating, managing or reviewing smart places. It provides guidance on managing data in accordance with the privacy legislation as well as in line with best practices and community expectations. Information about how to source additional advice if required is provided.

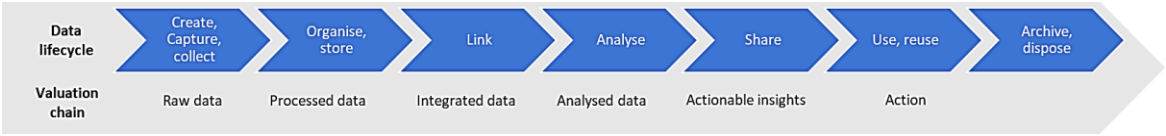
2. Protecting Smart Places Data

Smart places should be designed to avoid collection of personal information wherever possible. For some smart places initiatives, it may be necessary to collect personal information or collection of personal information may be incidental. The methods of data collection in smart places, including smart devices such as sensors or drones, the volume and frequency of data collected, and the defined spaces in which data is collected can contribute to the potential for individuals to be identified in the data, even if this is not the intention. For example, sensors placed on the exterior of houses to measure air temperature, may make it possible to identify when people are in or out of the house. The privacy impacts can be minimised by decreasing the frequency of data capture, aggregating the data to a street or suburb level when it is captured, or relocating sensors to less sensitive locations nearby (IoT Policy).

Avoiding collection of personal information or complying with privacy legislation if personal information is collected both present challenges in the smart places context. To assist with this, every NSW smart place or additional smart technology solution should be treated as a new project, and data protection principles, especially those relating to privacy and security, must be addressed from the start. The whole data lifecycle should be considered in smart places and as noted above, collection of personal information should be avoided wherever possible. To adopt a security- and privacy-by-design approach, smart places practitioners should consider:

- Undertaking a data needs assessment, which includes creating a business case to articulate the business outcomes and the data needed to achieve them.
- Consulting with community to understand their expectations about the collection and use of their data and the benefits of this to the community.
- Consulting with the Indigenous community about implementing Indigenous Data Sovereignty and Indigenous Data Governance in smart places initiatives
- Following privacy-by-design and security-by-design principles to ensure technology and data solutions have privacy and security built in.
- Conducting a Privacy Impact Assessment (PIA).
- Consulting with the IPC to seek advice on risks to privacy and information access rights.
- Creating secure digital services to protect government systems and data and complying with the NSW Cyber Security Policy.
- Considering the ethical implications of smart places initiatives, particularly the use of artificial intelligence.
- Conducting a pre-mortem exercise on every new and additional smart places project to identify vulnerabilities in the project and plan for unintended consequences.
- Referring to existing policies and frameworks including the IoT Policy and the Infrastructure Data Management Framework, for guidance on management and protection of IoT and infrastructure data

This section sets out best practices for protecting data across the stages of the data lifecycle as presented in the NSW Government Data Strategy.



References are provided to existing policies and guidance that can be applied in the smart places context.

2.1 Create, Capture, Collect

Data will be collected as part of the creation, management and use of smart technologies in smart places. This may include environmental data, operational data, and usage data. The analysis of these types of data can help generate insights to better manage the places and provide additional and better services to customers. It is recommended that personal information is not collected (unless necessary).

Best practice considerations for smart places practitioners when collecting data include:

- Minimising the personal information collected. Only collect what is needed, and do not collect personal information if the project does not require it. Avoid collecting fine-grain data that identifies specific detail like a residential address. Instead collect low grain data, like a suburb or postcode.
- Consider carefully whether any personal information could be inadvertently collected and if so, ensure compliance with the privacy laws or consider alternative solutions.
- Consider how government information that is collected can be proactively disclosed to citizens through project design.

Legal requirements if personal information is involved

Data collection must be lawful, direct, open and relevant (see guidance on IPPs and HPPs):

- Agencies must only collect personal information for a lawful purpose, which is directly related to the agency's function or activities and necessary for that purpose (IPP 1, HPP 1).
- Agencies must only collect personal information directly from the person concerned, unless the person has authorised collection from someone else, or if they are under the age of 16 and the information has been provided by a parent or guardian (IPP 2, HPP 3).
- Agencies must inform individuals that their personal information is being collected, why it is being collected, what it will be used for, who will have access to it, and how they can view or amend it before, or as soon as practicable after, their personal information is collected, unless the agency is exempt from doing so. This can be done using a Privacy Collection Statement, which in the smart places context may involve posting a prominent sign within the smart place or posting the notice on a related website or app (IPP 3, HPP 4).
- Agencies must only collect personal information that is relevant, accurate, complete, up-to-date and not excessive (IPP 4, HPP 2).

- Agencies also have responsibilities under the *Government Information (Public Access) Act 2009 (GIPA Act)*, notably:
    - data collected by a smart places project will be government information under the GIPA Act
    - the GIPA Act provides citizens with a right of access to government information unless there is an overriding public interest against disclosure
    - agencies should ensure that appropriate systems and processes are in place, including data governance frameworks and data storage and retrieval systems, to enable agencies to meet their obligations under the GIPA Act.

2.2 Organise, Store

Effective management, including the secure storage of Smart Places data is an important part of its protection. Consideration should be given to the type, frequency, volume and flow of data being collected, and these factors will inform the selection of appropriate transmission and storage methods. Data should be appropriately protected during transmission and at rest. Storage requirements may grow over time as Smart Places have the potential to generate large amounts of data, so development of storage models should be considered for longer term projects. Additional best practice data management and storage elements include:

- Selecting the most suitable storage option (cloud, government data centres and fog or edge computing) depending on your data requirements: How quickly insights are needed; type of data and bandwidth required; level of connectivity; level of security.
- Addressing privacy risks of transitioning to the cloud.
- Selecting appropriate methods of protection during transmission, such as using encryption or secure systems or protocols.
- Controlling who has access to data, including developing, implementing and enforcing robust user access rules and employing audit processes to verify authorised access and use of Smart Places data will support its protection. Access privileges should be routinely reviewed to ensure users have the least amount of permissions in order to perform their role.
- The data should be labelled in accordance with the NSW Government Information Classification, Labelling and Handling Guidelines.

Legal requirements if personal information is involved

Unless exemptions apply under law, personal or health information must be (see guidance on IPPs and HPPs):

- Kept securely, for no longer than necessary, and disposed of appropriately. It must also be protected from unauthorised access, use, modification or disclosure (IPP 5, HPP 5).
- Transparent to the person it is about so that they can find out what personal information about them is being stored, why it is being used and any rights they have to access it (IPP 6, HPP 6).

- Accessible by the person it is about and able to be updated, corrected or amended by the person when necessary (IPPs 7 and 8, HPPs 7 and 8).

2.3 Link, Analyse, Share, Use and Reuse

Smart places data will be used and shared to help make better decisions to improve the productivity, liveability and resilience of cities, towns and communities.

Wherever possible, Smart Places data will be released as open data and made available to the public in accordance with the NSW Open data Policy. This will increase government transparency and ensure the data is available for innovation by government, industry, researchers, and the community. Appropriate protections must be in place to ensure that individuals cannot be identified in any data that is released as open data.

Smart places data may also be shared between government agencies in accordance with the *Data Sharing (Government Sector) Act* and if personal information is shared, the privacy legislation also applies. Shared data may be combined or linked with other datasets and this may increase the risk of individuals being identified in the data. There may be opportunities to re-use smart places data for other purposes and care must be taken to ensure the privacy legislation is complied with if the re-use involves personal information.

To mitigate these risks, appropriate safeguards should be in place before using, re-using or sharing data. Ethical considerations should also be made before using smart places data in decision-making.

It is important to consider the following when using and sharing data collected from a smart place:

- Smart place practitioners should de-identify their data effectively. A practical and accessible guide has been developed by the Office of the Australian Information Commissioner and Data61.
- Follow the NSW data sharing principles and guidance on data sharing from Data.NSW and the Information and Privacy Commission to reduce the risk of a data breach or re-identification. Privacy preserving tools such as the Personal Information Factor (PIF) Tool have been used by NSW Government to assess the risk of identifying an individual in a dataset, including during the COVID-19 pandemic.
- Any Smart Place project using AI will follow the Mandatory Ethical Principles for the use of AI, unless certain exemptions apply. These principles can be applied to any project involving data-driven decision making.
- Smart places practitioners should include clauses in contracts to ensure that no personal information can be used or disclosed by service providers for a purpose other than what is specified in the contract and what is permitted by law.
- Care should be taken when transferring smart places data outside of NSW to ensure appropriate protection of the data in another jurisdiction.
- The data should be labelled in accordance with the NSW Government Information Classification, Labelling and Handling Guidelines.

Legal requirements if personal information is involved

Unless exemptions apply under law, personal or health information (see guidance on IPPs and HPPs):

- Must be accurate, relevant, up to date and complete before it is used (IPP 9, HPP 9).
- Can be used for the purpose for which it was collected, or for a directly related purpose which the person would expect. Otherwise, their consent to use the information for another purpose would generally be needed. Personal information may be used to prevent or lessen a serious or imminent threat to a person's health or safety (IPP 10, HPP 10).
- Cannot be disclosed unless it is for the purpose for which it was collected, or for a directly related purpose that the person was told about or would expect. Otherwise, their consent would generally be needed, and it is needed if the information being disclosed is sensitive personal information. Personal information may be disclosed if it is necessary to prevent a serious and imminent threat to any person's health or safety (IPPs 11 and 12, HPP 11).
- Can only be linked with the person's consent, unless exemptions apply (HPP 15). For personal information, a Public Interest Direction or Privacy Code may be needed.
- Should be transferred across borders in accordance with the IPC Guidance and for health information should comply with HPP 14.

2.4 Archive, dispose

Data generated from Smart Places projects should be retained and disposed of in accordance with an organisation's records and information management requirements. Regular disposal of data will have cost benefits and minimise data access and retention risks. It is recommended that needs assessments be undertaken from business, risk, accountability and customer perspectives to determine the appropriate retention or disposal strategies.

- The *State Records Act 1998* (NSW) sets the rules for how long government information needs to be retained. Depending on the business purpose of your project, smart places data will have different legal retention and destruction requirements. Refer to the NSW State Archives and Records website for more information.
- For data that is no longer required, delete or dispose of it at a set frequency, in accordance with the *State Records Act 1998* (NSW) and privacy legislation (IPP 5 and HPP 5).
- Data must be contractually required to be returned to government at the end of a contract, or when a service or relationship with a service provider is discontinued.

Legal requirements if personal information is involved

- Custodians of data and information must comply with the *State Records Act 1998* (NSW) which requires agencies to establish and maintain a records management plan and ensure appropriate records storage, maintenance and security and archiving of their custodial assets.

- Data must be destroyed in a manner appropriate for its sensitivity, with guidance found in the NSW Privacy legislation (IPP 5 and HPP 5), the *State Records Act 1998* and the NSW Government Information Classification, Labelling and Handling Guidelines.

3. Related Legislation, Policies and Documents

The NSW Smart Places Data Protection Policy acts as a way-finder for NSW Government agencies, to understand their obligations towards the collection, management, usage, storage, and deletion of data obtained as part of a smart place project in NSW. Further detailed information and resources are available below. This information may also be of interest to members of the public, local councils and service providers.

Issuer	Reference	Document Name
NSW Government	1998	*Privacy and Personal Information Protection Act 1998* (NSW)
NSW Government	2002	*Health Records and Information Privacy Act 2002* (NSW)
NSW Government	2009	*Government Information (Public Access) Act 2009* (NSW)
NSW Government	2018	Government Information (Public Access) Regulation 2018 NSW
NSW Government	1998	*State Records Act 1998* (NSW)
NSW Government	2015	*Data Sharing (Government Sector) Act 2015* (NSW)
Department of Customer Service	March 2021	NSW Government Internet of Things (IoT) Policy
Department of Customer Service	August 2020	NSW Government AI Strategy
Department of Customer Service	August 2020	NSW Government Artificial Intelligence (AI) Ethics Policy
Department of Customer Service	December 2020	NSW Government Infrastructure Data Management Framework (IDMF)
Department of Customer Service	July 2020	NSW Government's Smart Infrastructure Policy
Department of Customer Service	2020	NSW Government Cyber Security Policy
Department of Customer Service	2021	NSW Government Procure IT Framework
Infrastructure NSW	2018	NSW Government State Infrastructure Strategy
Department of Customer Service	2016	NSW Government Open Data Policy
Department of Customer Service	October 2020	NSW Government Cloud Policy
Department of Customer Service	2018	NSW Government Information Management Framework
Department of Customer Service	June 2013	NSW Data & Information Custodianship Policy

Issuer	Reference	Document Name
Department of Premier and Cabinet	November 2018	NSW Government Standard on Records Management
Department of Customer Service	February 2021	NSW Data Governance Toolkit
Department of Customer Service	June 2021	NSW Government Data Strategy
Information and Privacy Commission	May 2020	Fact Sheet - Information Protection Principles (IPPs) for agencies
Information and Privacy Commission	August 2019	Fact Sheet - The Health Privacy Principles (HPPs) guidance for agencies and organisations
Information and Privacy Commission	2016	Privacy Governance Framework
Information and Privacy Commission	April 2020	Fact Sheet - Reasonably Ascertainable Identity
Information and Privacy Commission	October 2020	Digital Projects for Agencies
Information and Privacy Commission	May 2021	Digital Restart Fund: assessing information access and privacy impacts
Information and Privacy Commission	June 2019	Fact Sheet - Consent and Bundled Consent
Information and Privacy Commission	May 2020	Fact Sheet – Digital records and the GIPA Act