NSW Smart Places Data Protection Policy

DRAFT

Document number: 1	Version number: 1
Date: Friday, June 18, 2021	

Contact details

Name: Alistair Tegart	Position: Principal Policy Officer, Data.NSW, NSW Data Analytics Centre (DAC)
Business Unit: Data, Insights & Transformation (DIT)	Division: Customer, Digital & Transformation (CDT)
Phone: 0414 191 047	Email: alistair.tegart@customerservice.nsw.gov.au

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 the 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 environment 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. The NSW Information and Privacy Commission has also 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 NSW Smart Places Data Protection Policy has been designed to make it easier for public and private sector smart places developers, managers and place owners to follow lawful and best practice data protection across the lifecycle of smart places data. The Policy requires these stakeholders to build data protection into smart places project design, and actively manage smart places data from collection to disposal.

This Policy is also designed to support the NSW Smart Places Customer Charter and help members of the public understand what it means for NSW Government to commit to treating data safely and securely and protecting personal information.

The primary users of this policy will be NSW Government agencies that are planning smart places projects, 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. In practical terms, personal information is any information that identifies an individual; it could include records with a name and address, photographs, video or audio footage, or fingerprints, blood or DNA.

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 under the PPIP Act or the Government Information (Public Access) Act 2009 (NSW) (GIPA Act). The Health Records and Information Privacy Act 2002 (HRIP Act) identifies Health Privacy Principles (HPPs) and specifies similar obligations to protect 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 technology is 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.

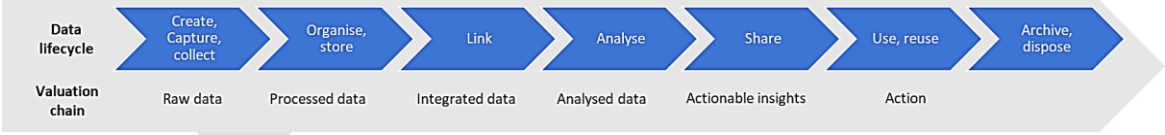
2. Protecting Smart Places Data

Ideally, smart places will be designed so that personal information is only collected with permission and a clear use. However, it may be necessary to collect personal information as part of a smart places initiative, or collection of personal information may be incidental. For example. if drones are used to collect data some personal information may be inadvertently collected.

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 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.
- 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.

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 automated 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 data 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.
- Being aware of the risks associated with combining data sources and the potential for individuals to be identified in the data.

Additional requirements if personal information is involved

- The relevant IPPs state that data collection must be lawful, direct, open and relevant.
- Agencies must obtain consent directly from the individual in question.
- Individuals must be informed before, or as soon as possible after, data collection has occurred through a Privacy Collection Statement.
- Organisations must minimize the amount of personal information collected only to what is needed for their purposes.

2.2 Organise, Store

Following established good data management practices enables better use of the data generated by Smart Places. The quality and accessibility of this data should be closely monitored by data owners and custodians. To align with best practice, Smart Place projects should:

- Follow good data management and governance practices.
- Clearly define roles and responsibilities for data ownership and management.
- Establish data governance contractually if there are third parties involved.
- Establish a data breach policy, and make staff aware of their responsibilities under it
- Contracts must ensure that no personal information can be used by a service provider for a purpose other than what is specified in the contract.
- Personal information must be automatically protected in systems so individuals do not have to take specific action to protect their privacy.
- The State Records Act notes that data custodians are responsible for creation, management, and protection of datasets even when these are delegated to another agency.

Additional requirements if personal information is involved

- Under the IPPs, data must be restricted, safeguarded, accessible and correct.
- Data must be protected from unauthorized access.

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 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.
- Selecting appropriate methods of protection during transmission, such as by the use of encryption or secure systems or protocols.
- Controlling who has access to data. Enforcing access rules and employing audit processes to verify authorized access and use of Smart Places data will support the protection of data.
- 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.

Additional requirements if personal information is involved

Unless exemptions apply under law, personal information must be:

- Kept securely, for no longer than necessary, and disposed of appropriately. It must also be protected from unauthorized access, use, modification or disclosure.
- Stored at the highest level of aggregation possible, and storage options will meet increased security requirements present under the PPIP Act.
- Be accessible, accurate, and able to be updated or amended when necessary.
- Contracts between government agencies and third-party service providers must include clear data storage requirements and adhere to the mandatory contractual framework for procuring ICT goods and services.

2.3 Link; Analyse; Share; Use and Reuse

NSW smart places data will be used and shared to help people and governments make better decisions about how to improve the productivity, liveability and resilience of cities, towns and communities. Wherever possible, NSW 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 authorised under the Data Sharing (Government Sector) Act. If personal information is shared, the privacy legislation applies. Shared data may be combined with other datasets and this may increase the risk of individuals being identified. To mitigate these risks, appropriate safeguards should be in place before sharing data. Ethical considerations should also be made before using smart places data in decision-making.

It is important to consider the following things 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.

Additional requirements if personal information is involved

- Under the IPPs, personal information can only be used for the purpose for which it was collected, unless certain exemptions apply.
- Personal information must not be disclosed unless certain exemptions apply.
- Personal information must be accurate, relevant, up to date and complete before it is used.
- Contracts must ensure that no personal information can be used by service providers for a purpose other than what is specified in the contract.

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.

Additional requirements if personal information is involved

- Data must be deleted as soon as the objective it was collected for is completed, noting that if it is a state record then additional considerations apply.
- 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.

- Data must be destroyed in a manner appropriate for its sensitivity, with guidance found the NSW Privacy legislation, the State Records Act (1988) and the NSW 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, members of the public, local councils and service providers 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.

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 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
Department of Premier and Cabinet	November 2018	NSW Government Standard on Records Management

Issuer	Reference	Document Name
Department of Customer Service	February 2021	NSW Data Governance Toolkit
Information and Privacy Commission	May 2020	Information Protection Principles (IPPs) for agencies
Information and Privacy Commission	2016	Privacy Governance Framework
Information and Privacy Commission	April 2020	Factsheet: 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