NSW GOVERNMENT | Customer Service

NSW Government Open Data Publishing Guidelines

Document number: V3.0	Date: 29 November 2022

November 2022

Table of Contents

1. Introduction

The NSW Government Open Data Policy promotes the release of NSW Government data for use by the community, researchers, businesses, and industry. The release of open data supports government transparency and accountability, provides a platform for innovation, and generates new insights to inform better public policy and services and deliver better outcomes for the community.

The NSW Open Data Policy sets out the principles for open data that open data should be:

- Open by default, protected as required
- Prioritised, discoverable and usable
- Primary and timely
- Well managed, trusted and authoritative
- Free where appropriate
- Subject to public input.

Release of open data by government means the community is well-informed and can make better decisions for themselves. However, there may be unintended consequences to releasing some data as open data, for example release of personal or otherwise sensitive information. Therefore, it is important to ensure appropriate safeguards are in place before data is released as open data.

The purpose of this document is to:

- Describe the open data publishing process
- Provide a clear approval process to follow for publishing open data
- Include guidance for publishing data in a digitally connected environment
- Describe roles and responsibilities for data custodians and other parties
- Mitigate risks associated with the publication of open data.

1.1 Open data and GIPA

The *Government Information (Public Access) Act 2009* (GIPA Act) establishes a proactive and open approach for the community to gain access to government information in NSW.

The premise of the GIPA Act is that disclosure of government information is in the public interest. All government agencies must disclose or release information unless there is an overriding public interest against disclosure. Only if there is an overriding public interest against disclosure should government information be withheld from the public (s 5).

To implement that presumption in favour of open government the GIPA Act sets out four information pathways:

- mandatory proactive release
- authorised proactive release
- informal access
- access applications.

Each pathway can be activated to open data. Likewise open data can be released absent the authority provided under the GIPA Act when it is truly open data. To assist agencies in identifying open data the Information and Privacy Commission (IPC) published a guide to open data.[1]

Fundamental to the obligation to release information is the overarching presumption in favour of disclosure of information. This is the starting point for all decisions regarding information access. When deciding whether to release information, decision makers must commence the public interest test from the position of acknowledging the presumption in favour of disclosure of information. Unless there is an overriding public interest against disclosure, agencies must provide the information. There are some limited exceptions to this general rule, for example, where dealing with an application would constitute a significant and unreasonable diversion of an agency's resources.[2]

The public interest test requires balancing factors for and against disclosure of each piece of government information. The IPC publishes a range of guidelines and factsheets to assist agencies to undertake the public interest test and balance the relevant factors.[3]

Agency decisions on open data – what and how to publish and in what form – should be made in consultation with the community, the research sector and industry. Community and industry feedback on the data should be published.

Public consultation on information release and related matters is required by the GIPA Act. The Information Commissioner has published a guide for agencies[4].

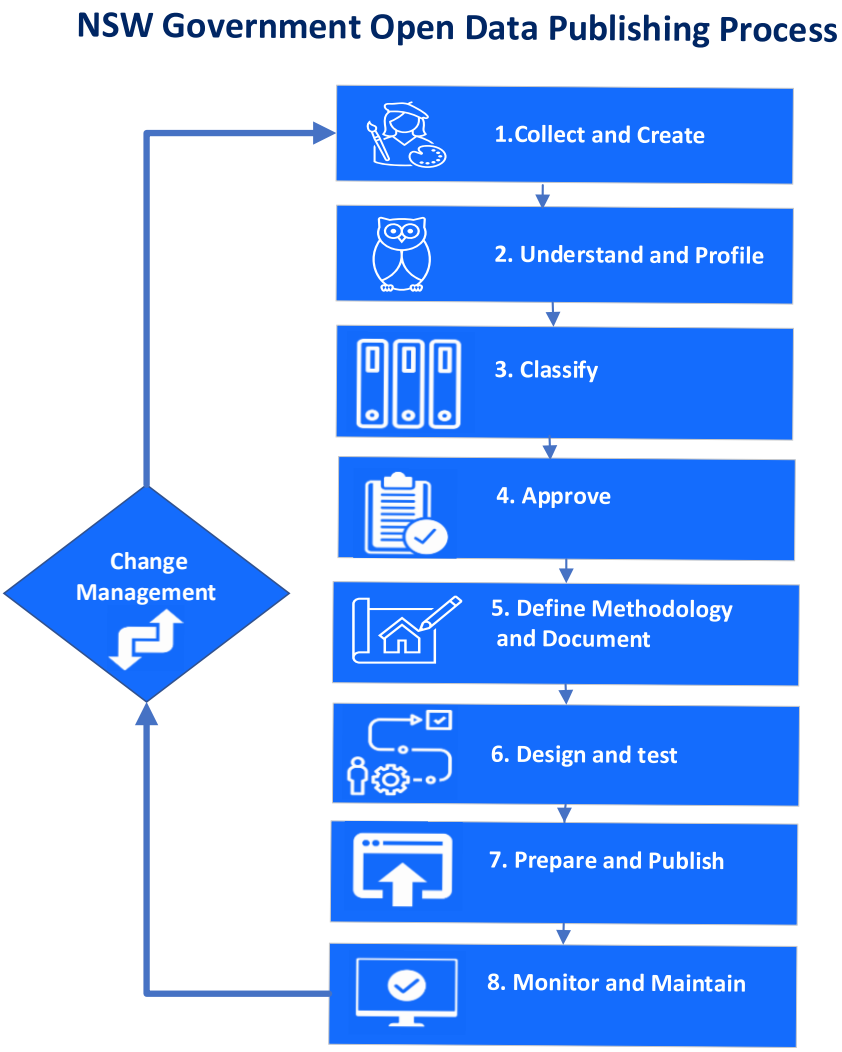
[1] Information Access Guideline 7: Open data (https://www.ipc.nsw.gov.au/information-access-guideline-7)
[2] IPC Factsheet: What is the public interest test (https://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test)
[3] https://www.ipc.nsw.gov.au/information-access/agencies/resources
[4] IPC Factsheet: Charter for Public Participation – a guide to assist agencies and promote citizen engagement (https://www.ipc.nsw.gov.au/sites/default/files/file_manager/Charter_for_Public_Participation_a_guide_to_assist_agencies_and_promote_citizen_engagement_June2018.pdf)

2. NSW Government Open Data Publishing Process

The NSW Government open data publishing process has eight steps which streamline the release of open data while minimising risks associated with releasing some data. Open data is not just about publishing static documents such as PDFs. It is also about publishing data that is dynamic, computer readable, accessible, and connected. This provides opportunities and flexibility for delivering excellent customer service and improving customer outcomes and innovation.

Publishing open data can be complex in a digital environment as often important datasets are published in multiple formats, on multiple media and platforms, and have APIs, forms, and connected applications. Figure 1 summarises the process for publishing NSW Government open data. Each step is described in detail and section 8 contains a complete check list.

Figure 1 NSW Government open data publishing process[5]



[5] Adapted from the Government of South Australia, Office of the Chief Information Officer (2014) "Open Data Process Guide"

2.1 Collect and create

The NSW Government Open Data Policy calls for data to be created and collected in ways that support downstream processing and release. Data collection processes need to follow legislative requirements which are discussed in more detail in 2.3 “Classify” section.

Key considerations for planning and designing a data collection or creation process include:

- Assign a data custodian with responsibility for the data
- Publish a data collection statement that informs people how their information will be used, including that it will be published, with appropriate safeguards
- Implement measures to ensure data quality and consistency such as field and cross field validation and use of standard data classifications
- Agencies should ensure at this stage that their agency information guide is also up to date in terms of documenting their information holdings.

Check list:

- ☐ Has a Data Custodian been assigned?
- ☐ Is there a data collection statement and does it cover release of open data?
- ☐ Are there data quality measures in place?

2.2 Understand and profile

Data that is of high public interest should be prioritised for release as open data. Understanding and profiling the data will inform whether it is suitable to release as open data and if so, ensure it is released with appropriate metadata, licensing and formats to facilitate its discovery and use.

Agencies need to check that the data has not already been released in response to a GIPA application. This should be recorded in the agency's disclosure log. Agencies should consider a process to systematise this step and feed this information into open data. This would also assist agencies to meet their review obligations under s7(3) of the GIPA Act.

Check list:

- Check data value – will the data be valuable and useful for the public? Have the public requested the data? Have they provided input into the release of the data?
- Has the data already been released in response to a GIPA application?
- Profile and describe the data examining the structure, content and relationships. Document field labels, data type, data model, dataset current size and potential size. Check data quality and if poor the data should not be published until data quality has been improved. Determine if there are any free-text or comments fields that could contain sensitive information. Remove any ID fields that could possibly linked to other datasets, making it more likely for the data to be re-identified.
- Consult with the Subject Matter Expert to check the data content is as expected.
- Ensure that there are no legal restrictions preventing the publication of the data. Include an assessment by the GIPA officer where the agency considers that there may be factors against the disclosure of the information.
- Check that the data collection statement allows for the public release of the data.
- Consider authorised proactive release under the GIPA Act – s7 of the GIPA Act authorises and encourages agencies to make any government information held by an agency publicly available unless there is an overriding public interest against disclosure. The agency should apply the public interest test under s13 to determine whether the data can be proactively released. The IPC has published a self-assessment checklist to help agencies identify the information that can be released proactively.
- Ensure that due diligence is conducted to confirm your agency owns the data and has the right to publish it, including checking that there are no third-party rights to the data.
- Assign a license type, Creative Commons licenses are recommended for open data.

2.3 Classify

The NSW Open Data Policy states that data should be open by default, protected as required. Therefore, before publishing data as open data, it is important to determine if the data needs to be protected.

This can be done by considering whether the data to be published is sensitive in any way. For example, whether it includes information that may impact things such as security, privacy or business confidentiality.

Even if data is generally considered to be already in the public domain it may be sensitive depending on the context of the data and its use. For example, every instance of the data may not be in the public domain and bringing this data together in a searchable, machine-readable dataset may increase its sensitivity.

Safeguards for protecting data before it is released may include anonymisation, aggregation, using synthetic data or suppressing data. Guidance on understanding specific safeguard requirements and making data safe for publication is available at: https://data.nsw.gov.au/making-data-safe-sharing.

Security

Compromise, either deliberate or accidental, of sensitive or security classified information could result in harm to an individual, organisation or government.

All NSW Government data should be classified according to the NSW Information Classification, Labelling and Handling Guidelines and sensitive information must not be published as Open data. Appendix 1 of the NSW information Classification, Labelling and Handling Guidelines provides a Business Impact Levels tool which can be used to determine the level of sensitivity of information. Impacts could be to:

- Dignity or safety of Individuals
- Entity operations, capability and service delivery
- Entity assets and finances (operating budget)
- Certain infrastructure
- International relations
- Crime prevention, defence or intelligence operations
- Contracts and agreements
- Information under legal professional privilege
- Economy
- Policies and legislation.

Handling practices outlined in the NSW Government Information Classification and Labelling Guidelines should be followed for sensitive information.

Data may be able to be published if appropriate safeguards are applied. Some approaches for making data safe for publication are available at: https://data.nsw.gov.au/making-data-safe-sharing.

Privacy

Personal or health information should never be published as open data. This may include data with direct identifiers (such as name) or data where identification is possible through a combination of characteristics included in the dataset or if the dataset is combined with another dataset. Consider whether further information is needed on the risks of re-identification and the limitations of de-identification techniques. Further information about how to de-identify personal information can be found at: https://www.ipc.nsw.gov.au/fact-sheet-de-identification-personal-information.

Personal information is defined in the Privacy and Personal Information Protection Act 1998 (NSW) and health information is defined in the Health Records and Information Privacy Act 2002 (NSW).

Examples of personal information include a record which includes an individual's name and address, photographs, images, video or audio footage and fingerprints, blood or DNA samples. Other examples of personal information include credit card number, Medicare number and driver license number.

Consideration of the risk of identity theft, financial, physical or psychological harm and reputation of an individual should be made before a dataset is published as open data. A privacy impact assessment (PIA) can be completed to determine if personal or health information is included. Information on PIAs can be found on the IPC website: https://www.ipc.nsw.gov.au/guide-privacy-impact-assessments-nsw.

If personal or health information is identified in the data, a range of mechanisms can be used to safeguard the data and remove its sensitivity, so that it may be able to be published. Some approaches are available at: https://data.nsw.gov.au/making-data-safe-sharing.

Data which does not contain personal information may still have the potential to impact on individuals. Publication of open data may reveal information which could result in a security or other risk to an individual. For example:

- Individual or low volumes of aggregated data records in public transport datasets could potentially reveal the travel routes of small groups of individuals which poses a safety risk
- Publication of location information for certain types of business premises or health services may expose individuals to security risks.

The examples above would not be released as open data. Noting that operational data may need to be granular to be effective – not just aggregated. For example, real-time locations of public transport vehicles where there is no privacy risk.

Department of Customer Service (DCS) has used the Personal Information Factor tool to safeguard data on COVID cases published on the Data.NSW open data portal.

Ethics

Consider data ethics before making the decision to publish data as open data. Consider if there are any cultural considerations relevant to this data, is the data likely to impact people or communities? or will publishing the data impact the environment?[6]

Society and the natural environment

Community input is important when deciding to release open data. Consideration of whether the data includes information that may identify a community or group should be made. This may include children and young people, aboriginal peoples, multi-cultural communities, refugees, people experiencing homelessness or domestic violence, and people in the justice system.

These communities or groups should be involved in any decision to release data that identifies them. Consideration of whether release of the data could have an impact on the environment should also be made. For example, data that reveals the location of endangered or protected species that may be more at risk if their habitat is revealed.

Business confidentiality

Consideration should be given to whether a dataset contains commercially sensitive information such as information that could impact a businesses' competitiveness or viability or influence the financial markets. This may include information about intellectual property, trade secrets, credit scores, plans for mergers.

Although some information about businesses may be in the public domain, this information could be considered sensitive, depending on the context of the data and its use.

Safeguards for protecting sensitive data may include anonymisation, aggregation, using synthetic data or suppressing data. Guidance on understanding specific safeguard requirements and making data safe for publication is available at: https://data.nsw.gov.au/making-data-safe-sharing.

[6] Adapted from Open Data Institute (2022), "Assessing risk when sharing data: a guide" https://theodi.org/wp-content/uploads/2022/02/Assessing-risks-when-sharing-data-a-guide-OPEN.pdf

Checklist

- Ensure that there is no sensitive information included. Check the Information Classification (NSW Government Information, Classification, Labelling and Handling Guidelines) and consider any risks to individuals, communities, the environment or businesses
- Ensure that there is no personal or health information included in the data
- Apply safeguards to the data to make it safe for public release and ensure health/personal and sensitive information is not released.

2.4 Approve – open data approval process

Before publishing an NSW Government dataset as open data, approval must be obtained from the Executive Director of the business unit that has custody of the data. Aggregated or linked datasets may have a different data custodian to that of the original dataset and care should be taken to check who the relevant data custodian is.

The approval process must be undertaken to ensure that all risks have been assessed and all processes have been developed and tested prior to approval for the data to be published as open data.

Table 1. Open data approval process

Step	What is being approved	Role responsible*
1: Collect and Create	Collection of the data The data collection statement	The Data Authority Legal Advisor
2: Understand and Profile	The description of the data and data model.	Subject Matter Expert
3: Classify	The data is classified according to the NSW Government Classification, Labelling and Handling Guidelines. The data is not sensitive, does not contain personal or commercially sensitive information.	Data Custodian
4: Approve	Oversight of the steps above. Approve publication of the open data.	The Data Authority is required to approve the release of the dataset based on the information provided by the Subject Matter Expert and the Data Custodian. Note: Aggregated or linked datasets may have a different data custodian.
5: Define Methodology and Document	The data format, frequency of release, method of delivery, metadata and data dictionary.	Data Custodian
6: Design and test	The design of the data pipelines and APIs Data visualisations Successful testing	Business System Owner
Final Approval	Approval of final open data products	The Data Authority

*Note: Data roles and responsibilities are described in section 3.

Checklist

- ☐ Has approval for publication of the dataset been given, based on:
  - ☐ There is a public interest in the release of the data
  - ☐ The data been assessed, and it has been confirmed that it does not contain health/personal or otherwise sensitive information
  - ☐ Third-party rights been determined and considered
  - ☐ A data licence type has been applied (for example: Creative Commons licence)
  - ☐ Metadata and a data quality statement have been developed

2.5 Define Methodology and Document

Open data may be released using several different methodologies and channels including via direct upload to an open data portal, through API, connected applications, forms, maps, webservers, and infographics.

Defining the methodology for data delivery and documenting how the data flows between data collection points to data publishing points is important for ongoing data management, data security and governance purposes.

This will ensure safeguards applied to open data are maintained and that no sensitive data is inadvertently introduced into data that has been released as open data.

Documentation to be maintained by the Data Custodian:

Direct data uploads – Document the location and details of direct data uploads made for publication of open data. Often one dataset is uploaded to several different locations and if updates are made, each of these locations will then need to be updated.

Automated data uploads – Documentation including diagrams of data pipelines are required. This documentation must describe data ingestion, transformation, frequency of update, if copies of the data are made and stored, which systems are used and where the data is being published, particularly if the data pipeline is publishing to multiple channels.

Application Programming Interface (API) – An API is a software go-between that allows two applications to talk to each other. When APIs are developed to publish open data, technical details need to be documented. Documentation is to include the URL, a description of what the API does, the parameters, schemas, if a key is required and expected response. Include examples of API requests, responses and messages as well as versions.

Downstream documentation of connected applications. Recognising that because the data is open, not all downstream connected applications will be known, internal connected applications (i.e., those within NSW Government), forms and processes must be documented. This is so that when changes are made to the data, schema or calculations, downstream impacts can be gauged.

Checklist

- ☐ Have open datasets that are directly uploaded for publication been documented?
- ☐ Have data flows from data collection to data publishing points been documented?

2.6 Design and test

As systems and applications become more complex over time it is more important than ever to focus on good data design and testing data and data products prior to publishing open data. For example, open data has been used in mobile applications built for smart phones. Testing allows for validation of the data, and data products such as data visualisations, and it allows the Subject Matter Expert and the Data Custodian to view the data after it is processed by the system or application to confirm the data is as expected.

Design of automated data delivery methods and testing of these to ensure that the code is correct, and that quality control and assurance processes have been incorporated into the code are key to providing accurate, good quality open data.

Checklist

- Is there a test plan which is designed to test data and data products?
- Are the data schemas, calculations, and data products, correct?
- Have data pipelines been tested and the data validity checked?
- Have checks been designed to flag if the code fails to run?
- If code is preforming multiple tasks, have the results been checked to make sure they produce the same result as if they were being executed one after the other?

2.7 Prepare and Publish

The NSW community are interested in data, especially data that is relevant to current issues such as emergency situations. Their data and technology skills range from foundational to advanced. To meet community demand, it is important that data is published in multiple formats, enabling the community to access data that suits their needs. The data must be reliable, well managed and well described, and there needs to be a way for the public to seek clarification or request data.

Before open data can be released it needs to be documented including the collection method, transformations, and data quality.

The information below will contribute to the metadata statement that must be published with the open data.

- Description of the dataset
- Date of release
- Format of the data to be released. Multiple formats are encouraged as are formats that are machine readable
- Frequency of updates
- Including a data dictionary is best practice
- Data quality statement – The tool to help create a data quality statement can be found here.

Checklist

- ☐ Has a metadata statement been written?
- ☐ Has a data quality statement been developed?
- ☐ Is there a data dictionary?

2.8 Monitor and Maintain

Data published as open data may change over time. Publication of open data should never be “set and forget”, especially when publication processes have been automated.

If changes are to be made to the dataset, an assessment of the impact of those changes should be made before they are implemented. This should include conducting a sensitivity and privacy assessment as well as testing proposed changes in test environments. The metadata and data quality statement for the dataset should be updated by the data custodian.

Datasets should be monitored for changes to the data model or volume of data, both of which may indicate an unexpected change. If such changes are identified, the dataset should be removed from public access until such time that the changes have been assessed and approval for the new version has been obtained from the Data Authority.

The changes and any associated risks should be communicated to relevant stakeholders, including the Data Publisher.

The Data Publisher is responsible for monitoring data use over time and collation of customer feedback. This information is to be provided back to the Data Custodian. The Data Publisher has responsibility for monitoring the publication process and system performance.

Information to be maintained by the Data Publisher:

- Number of direct data downloads and name of datasets that are being accessed
- Number and type of API calls that are being made
- Monitoring of search terms used to find the data
- Monitoring of channel usage
- Monitoring of public comments and feedback and requests for data.

Checklist

- ☐ Does the Data Custodian regularly check published data and monitor for changes?
- ☐ Does the Data Publisher monitor data use?
- ☐ Does the Data Publisher monitor customer feedback?
- ☐ Are mechanisms in place to flag when data models change?

3. Data Roles and Responsibilities

Table 2 describes the roles, functions and responsibilities to enable the release of open data.

Table 2. Open data roles, functions and responsibilities

Role	Function	Responsibilities
Data Authority	• has administrative or legislative responsibility for a specific government business function to which the data is integral (e.g. an Executive Director or above depending upon the risk) • has the authority to collect the data • has responsibility for the existence, protection and use of the dataset.	• must understand and approve the collection of data including the data collection statements • lead and champion the data prioritisation and release program for their Business Unit or Branch • must approve the release of the data and provide due diligence oversight of the open data process for the dataset they are responsible for • the Data Authority responsible for publishing the data may not always be the same one that approved the collection of the data. The Data Authority approving publication must have knowledge of the data collection process • may seek further approval or consultation if the dataset has a high public interest or has cross agency relevance.
Data Custodian	• manages the data • has technical knowledge of databases and information systems • has knowledge of the data dictionary, data schema, and calculations.	• developing, managing, care and maintenance of a specified dataset or information asset • ensuring that all legal, regulatory and policy requirements are met in relation to the management of the specified dataset or information asset • determining the conditions for appropriate use, sharing and distribution of the specified dataset or information asset enable and/or implement data release • maintain metadata about each dataset or information asset for both management and dissemination purposes.
Subject Matter Expert	• has technical, detailed knowledge of the data.	• monitors changes and updates to the subject matter and communicates to the data custodian and business system owner if any changes will impact the data collection or interpretation • undertakes regular review activities and ensures open data is updated • responds to enquiries relating to the data once published.

Role	Function	Responsibilities
Business System Owner	• has operational oversight of technology or applications.	• assigning the role of data custodian for all information and data assets relevant to their business • ensuring technology resources support the collection or creation and management of data.
Data Publisher	• has responsibility for publishing the open data as specified by the data custodian.	• is delegated the responsibility for distributing the data through a channel or service such as an open data portal, application, or website • is responsible for monitoring the use, data access and public response to the data • The data publisher can unpublish data if the data is later found to be of poor quality or contain sensitive or personal information. This will be done in consultation with the data custodian.
Legal Advisor	• legislative interpretation and advice.	• advises on data collection statement and privacy statements • provides legal advice in relation to specific legal restrictions of data distribution • provides legal advice in regard to intellectual property rights that subsist in any third-party material.
Cyber Security Advisor	• Agency Cyber security advisor.	• provides advice on the NSW Cyber Security Policy.

4. Data Incident Management

Despite best efforts to safeguard open data, personal or otherwise sensitive data may be released. It is important to manage this as quickly as possible to minimise harm to individuals, businesses, the environment or government. Agencies should follow their data incident management plan. The IPC has published Data Breach Guidance for NSW Agencies.

Agencies that identify a data incident must inform the data custodian and data publisher immediately.

If, despite the best efforts of agencies, open data does result in the disclosure of personal or health information, the agency should notify the Privacy Commissioner and, where possible, the individual whose information has been disclosed.

5. Training

The Information and Privacy Commission (IPC) provides an eLearning Module on Open Data. Anyone involved in release of Open data should complete this training.

1. Go to the IPC eLearning Portal: https://elearning.ipc.nsw.gov.au/
2. Either log in, or if you are not already registered, sign up to use the portal
3. Complete the Open data training
4. Download your certificate.

6. Useful Resources

The following resources and references are available:

NSW Government Open Data Policy

https://data.nsw.gov.au/making-data-safe-sharing.

NSW Government Information Classification, Labelling and Handling Guidelines

IPC Open data training: https://elearning.ipc.nsw.gov.au/

IPC data breach guidelines: https://www.ipc.nsw.gov.au/data-breach-guidance-nsw-agencies

IPC public interest test: https://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

7. Publishing Process and Risk Mitigation

NSW Open Data Publishing Process	Risk being mitigated
1: Collect and Create	• The person providing the data is not aware that the data will be published • The data collected is of poor quality making downstream processing and release difficult.
2: Understand and Profile	• Accidental release of data that contains personal information or can be re-identified • Accidental release of data that contains sensitive information.
3. Classify	• Accidental release of data that contains personal information or can be re-identified • Accidental release of data that contains sensitive information.
4. Approve	• Accidental release of data that has not been approved for publication.
5. Define methodology and document	• Lack of information regarding data collection and publication processes making it difficult to track if there is an issue with the data.
6. Design and Test	• That planned open data products, once processed through code, systems, and calculations, are published in a suitable format.
7. Prepare and Publish	• Potential for accidental misinterpretation of data • Potential for malicious inference.
8. Monitor and Maintain	• Accidental release of data that has not been approved to be open.

8. Check List

NSW Open Data Publishing Process	
Tick box	**1. Collect and Create**
☐	Has a Data Custodian been assigned?
☐	Is there a data collection statement and does it cover release of open data?
☐	Are there data quality measures in place?
	2: Understand and Profile
☐	Check data value – will the data be valuable and useful for the public. Have the public requested the data? Have they provided input into the release of the data?
☐	Has the data already been released in response to a GIPA application?
☐	Profile and describe the data examining the structure, content and relationships. Document field labels, data type, data model, dataset current size and potential size, data quality. Determine if there are any free-text or comments fields that could contain sensitive information.
☐	Consult with the Subject Matter Expert to check the data content is as expected.
☐	Ensure that there are no legal restrictions preventing the publication of the data. Include an assessment by the GIPA officer where the agency considers that there may be factors against the disclosure of the information.
☐	Check that the data collection statement allows for the public release of the data.
☐	Consider authorised proactive release under the GIPA Act – s7 of the GIPA Act authorises and encourages agencies to make any government information held by an agency publicly available unless there is an overriding public interest against disclosure. The agency should apply the public interest test under s13 to determine whether the data can be proactively released. The IPC has published a self-assessment checklist to help agencies identify the information that can be released proactively.
☐	Ensure that due diligence is conducted to confirm your agency owns the data and has the right to publish it, including checking that there are no third-party rights to the data.
☐	Assign a licence type, Creative Commons licenses are recommended for open data.
	2. Classify
☐	Ensure that there is no sensitive information included. Check the Information Classification (NSW Government Information, Classification, Labelling and Handling Guidelines) and consider any risks to communities, the environment or businesses.
☐	Ensure that there is no personal or health information included in the data.
☐	Apply safeguards to the data to make is safe for public release and ensure personal and sensitive information is not released.
	4. Approve
☐	Has approval for publication of the dataset been given?
	5. Define methodology and document
☐	Have open datasets that are directly uploaded for publication been documented?
☐	Have data flows from data collection to data publishing points been documented?
	6. Design and Test
☐	Is there a test plan which is designed to test data and data products?
☐	Are the data schemas, calculations, and data products, correct?
☐	Have data pipelines been tested and the data validity checked?
☐	Have checks been designed to flag if the code fails to run?

NSW Open Data Publishing Process	
☐	If code is preforming multiple tasks, have the results been checked to make sure they produce the same result as if they were being executed one after the other?
	7. Prepare and Publish
☐	Has a metadata statement been written?
☐	Has a data quality statement been developed?
☐	Is there a data dictionary?
	8. Monitor and Maintain
☐	Does the Data Custodian regularly check published data and monitor for change?
☐	Does the Data Publisher monitor data use?
☐	Does the Data Publisher monitor customer feedback?
☐	Does the Data Publisher have mechanisms in place to flag when data models change?

9. Document Version Control

Version	Date	Prepared by	Comments
1.0	August 2022	Elizabeth de Vries	Final draft incorporating working group comments.
2.0	September 2022	Elizabeth de Vries	Incorporating comments from IPC
3.0	November 2022	Elizabeth de Vries	Incorporating comments from Transport NSW

Customer, Delivery & Transformation

Address: McKell Building 2-24 Rawson Place, Sydney NSW 2000

www.customerservice.nsw.gov.au