

3. Legal and Policy Context

The Toolkit has been designed to support NSW Government agency compliance with relevant all-of-government statutes, policies and frameworks that relate to the collection of data, data management and retention, confidentiality, data sharing, data linkage and public release.

3.1 Legislative requirements

Legislative instruments relating to the Toolkit include:

- ***Government Information (Public Access) Act 2009 (NSW)***

The [GIPA Act](#) facilitates public access to NSW Government information. It does this by authorising and encouraging the release of information by NSW Government agencies, giving members of the public the right to request access to government information, and by ensuring government information is only restricted where there is an overriding public interest against disclosing the information.

- ***Privacy and Personal Information Protection Act 1998 (NSW)***

The [PPIP Act](#) provides for the protection of personal information, and the protection of the privacy of individuals generally. Under the Act, all personal information that is made, kept or collected by government organisations must be created and managed in accordance with the Information Protection Principles under the PPIP Act. The Information and Privacy Commission website has an overview of [NSW privacy legislation](#).

- ***Health Records and Information Privacy Act 2002 (NSW)***

The [HRIP Act](#) protects health records and information by protecting the privacy of an individual's health information held by the public and private sectors, enables individuals to gain access to their information and provides an accessible framework for the resolution of complaints regarding the handling of health information. The 15 [Health Privacy Principles](#) are legal obligations that agencies must abide by when collecting, holding, using and disclosing a person's health information.

- ***State Records Act 1998 (NSW)***

The [State Records Act](#) sets out the rules for the creation, capture, control, use, maintenance and disposal of all records and information in line with whole-of-government records and information management policies. The NSW State Archives & Records Authority has developed the [Records and Information Management Policy checklist](#) that

helps agencies ensure their internal strategies are consistent with whole-of government information management policy.

- ***Data Sharing (Government Sector) Act 2015 (NSW)***

The [Data Sharing Act](#) enables the sharing of data between NSW Government agencies, and with the Data Analytics Centre (DAC). The Act encourages and facilitates data sharing, outlines safeguards for sharing data, states that data sharing must be legally compliant, ensures data involving personal information is protected, and allows the responsible Minister to direct agencies to provide data to the DAC under certain circumstances.

3.2 Policies and other guidance

Policies and other guidance relating to the Toolkit include:

- ***NSW Open Data Policy***

Data should be open to the extent that its management, release and characteristics meet the objectives of openness, accountability, fairness and effectiveness set out in the *Government Information (Public Access) Act 2009* (NSW). Under the GIPA Act, there is a presumption in favour of the disclosure of information, unless there is an overriding public interest against disclosure.

The Policy sets out [six open data principles](#) that all government data must be:

1. Open by default, protected where required;
2. Prioritised, discoverable and usable;
3. Primary and timely;
4. Well managed, trusted and authoritative;
5. Free of charge where appropriate; and
6. Subject to public input.

- ***NSW Cyber Security Policy***

The [Policy](#) sets out mandatory requirements that all agencies must comply with to ensure that cyber security risks to data, information, and systems are managed and data is kept secure. These include: implementing cyber security and governance; building and supporting a cyber security culture across the agency; managing cyber security risks and reporting against the Cyber Security Policy Requirements.

- ***NSW Data and Information Custodianship Policy***

The [Policy](#) defines a set of principles for the management and maintenance of the State's core data and information assets as well as outlining custodianship roles and responsibilities. Implementation of this policy and adherence to its principles facilitate compliance with the NSW Information Management Framework.

- ***NSW Information Management Framework***

The [Framework](#) sets out the core characteristics of 'information' for the NSW Government, which includes data and records, as well as a shared whole-of-government direction for information management. It sets out the vision, principles, minimum requirements, governance and capabilities for effective information management across the public sector. The Data Governance Toolkit expands on the data governance-related components of the Framework.

- ***NSW Information Classification, Labelling and Handling Guidelines***

The [Guidelines](#) set out the NSW Government's approach to classifying, labelling and handling sensitive information. The classification of information created, owned and managed by the NSW Government is a mandatory requirement under the NSW Cyber Security Policy. The Guidelines are consistent with the Australian Government security classification system.

Additional legal, regulatory and policy requirements may apply in specific agency or business domains. All organisations should identify the specific requirements that apply to their environment.

3.3 State, National and International standards

State, National and International standards already exist with respect to data governance. All NSW public sector agencies are responsible for conforming to appropriate standards, including those issued by State Records NSW and the Information and Privacy Commission NSW.

Standards specific to data management are included in the Data Management component of this Toolkit and are based on the internationally recognised Data Management Body of Knowledge guide.¹

¹ DAMA Guide to the Data Management Body of Knowledge, Edited by M. Brackett, S. Early and M. Mosley. Bradley Beach, NJ: Technics Publications LLS, 2017 (second edition)

While this Toolkit will be updated to reflect ongoing developments in standards and best practice, public sector agencies are expected to maintain their understanding of current applicable standards.