



Policy Title	Data Governance Policy
Related Documentation	Data Breach Policy Procurement Policy NSW Government Open Data Policy
Relevant Legislation	<i>Government Information (Public Access) Act 2009</i> <i>Data Sharing (Government Sector) Act 2015</i> NSW Government Data Strategy
Responsible Officer	Manager Corporate Strategy and Insights

**UNCONTROLLED WHEN PRINTED**

**Objective**

1. This Policy has the following objectives:
  - (a) Support processes to govern and protect Council data and data assets.
  - (b) Define roles and responsibilities regarding Council data governance.
  - (c) Ensure Council can leverage the value of its internal data, external data, as well as data and insights derived through consultancies.
  - (d) Ensure effective records regarding data access, reporting, managing, sharing, and storage.
  - (e) Ensure Council complies with relevant laws, regulations, and standards.

**Policy Statement**

2. This Policy has been developed to strengthen data governance practices, so that Council can best leverage the benefits of its data assets and manage associated risks. This is pertinent given the ever-increasing speed, variety, and volume of data, and the expectations on government agencies to strengthen evidence-based decision making.
3. This Policy describes principles for governing the quality, storage, security, and usage of data assets across the full data lifecycle. This includes outlining the roles and responsibilities of Council staff, contractors, and consultants regarding access, sharing, storage, disposal, and backup of Council data assets.

**Scope**

4. This Policy applies to all inbound and outbound data assets directly associated with Council activities. This includes:
  - (a) All data assets used in the administration of Council. This includes data in any format (e.g., electronic, print, archived).

<b>DATA AND DOCUMENT CONTROL – GOVERNANCE USE ONLY</b>		
<b>Directorate:</b> City Planning & Corporate Services	<b>Adopted Date:</b> 10/12/2024	<b>Page:</b> 1 of 4
<b>Section:</b> Corporate Strategy & Insights	<b>Revised Date:</b> 10/12/2024	
<b>Record No:</b>	<b>Minute Number:</b> 373	
	<b>Review Date:</b> 30/12/2027	

(b) All data and insights generated/produced through external consultancies.

5. This Policy applies to all Council staff, contractors, and consultants as per points 4a and 4b.

**Definitions**

<b>Term</b>	<b>Definition</b>
Data	Measurements or observations collected as a source of information that can be communicated, stored, and processed.  Data generally refers to facts and figures represented as numbers, text, graphics, sound or video. Data can take different forms and pertain to a range of topics or areas.
Council Data	Any data created, received, maintained, and/or communicated by Council. This includes data and insights that are generated/produced by third parties (e.g., consultants) through Council contracts.
Data Asset	A data asset is a structured collection of data. It can include raw data, metadata, models, algorithms, research reports, visualisations and analyses etc.
Data access	The right to read, copy, or query data.
Data Owner	Council staff member responsible for the governance of one or more Council data assets.
Data sharing	The exchange of data between entities. Restrictions and controls imposed are contingent upon the data's sensitivity and privacy impact.
Data Specialist	Business and technical subject matter expert in relation to a data/information asset and/or data analyses more broadly.
Data User	Any staff member, contractor, or consultant who accesses, modifies, or analyses Council data as part of their day-to-day activities. All Data Users must comply with this Policy.

**Legislative Context**

6. The NSW Government Data Sharing Act aims to facilitate sharing of government sector data between agencies, in order to:
  - (a) Support good Government policy making, program management, and service planning and delivery.
  - (b) Provide protections and safeguards for data sharing.
7. The NSW Government Open Data Policy assists NSW Government agencies to:
  - (a) Release data for use by community, research, business, and industry.
  - (b) Embed open data into business-as-usual.
  - (c) Support the *Government Information (Public Access) Act 2009*.

**Principles**

8. Data Management and Use
  - (a) Council data assets must be:

- i. Actively managed throughout the data lifecycle (from collection/creation through to disposal).
- ii. Used to support Council's efforts to meet its strategic goals and objectives (including strategies and objectives in the Community Strategic Plan).

9. Roles and Responsibilities:

- (a) The Executive Team has overall responsibility for data management planning and improvement. This includes:
  - i. Assigning staff to be Data Owners for corporate datasets and systems.
  - ii. Providing appropriate resources to manage corporate data and data systems.
  - iii. Resolve any issues escalated by Data Owners and Data Specialists.
- (b) Data Owners are responsible for the oversight of administrative and governance issues relating to assigned data assets. This includes:
  - i. Ensuring effective local protocols are in place to guide the appropriate use of the respective data asset.
  - ii. Implementing business processes to ensure appropriate data governance, including maintaining data quality and integrity.
  - iii. Considering requests for disclosure of corporate data assets in accordance with this policy, relevant legislation, and third-party data sharing agreements.
  - iv. That all regulatory, legal, and policy requirements are met in relation to the data asset.
  - v. Providing appropriate training for current and potential users before granting systems and data access.
  - vi. Authorise and monitor the secure use of data assets within their functional areas to ensure appropriate access, accuracy, classification, privacy and security.
- (c) All Data Users (including internal staff and external contractors) and Data Specialists are responsible for complying with this policy.

10. Classification and Security:

- (a) Data security measures must be followed at all times.
- (b) Personal use of any Council data is prohibited.
- (c) Appropriate safeguards must be in place to manage access and use of data in all formats.
- (d) Any data breaches must be addressed as per the Data Breach Policy.

11. Data Sharing and Procurement

(a) **Data access and use within Council.**

- i. The Data User must seek formal written approval from the respective Data Owner.
- ii. The Data Owner must consider the request in a timely manner, and – depending on appropriateness and plausibility – provide the Data User with systems access or summary data.
- iii. Executive approval may be required depending on the sensitivity of the corporate data and/or the importance of the data request.

**(b) Data sharing and release for use outside of Council.**

- i. The data assets to be shared must be consistent with the principles of the NSW Government Open Data Policy; that is, to inform good Government policy making, program management, and service planning and delivery at Campbelltown City Council.
- ii. The Data User (e.g., a project manager) must seek written approval from the Data Owner. In situations where the data assets are considered sensitive (as determined by the Data Owner), written approval is required from Council Executive. All relevant stakeholders must consider the request in a timely manner and provide a decision with respect to the appropriateness and plausibility of sharing the data (or granting systems access).
- iii. Data sharing arrangements must be reflected by being included in relevant contracts specifying rules around use, security, and disposal of corporate data.

**(c) Data and insights derived through Consultancies.**

- i. As per Council's Procurement Policy, Council can engage third parties for consultancy activities. Often these consultancies generate new data, information, and/or insights that are value for Council and the broader community.
- ii. Consultancy contracts must ensure Council is provided with all data files generated through such consultancies, as well as relevant metadata, derived insights, and analytic approaches.
- iii. Data repositories used by/during a consultancy must be located within Council's ICT environment unless this should act as a barrier to the execution of these consultancy services.
- iv. The above information must be provided to Council in a timely manner and in an appropriate format.

**Effectiveness of this Policy**

12. This Policy will be reviewed every 3 years.

**END OF POLICY STATEMENT**