Organisational policy

Information Access and Management

Corporate Plan reference	An outstanding organisation – A high performing, customer-focused organisation marked by great people, good governance and regional leadership.	
Endorsed by Chief Executive Officer		
Manager responsible for policy	Chief Information Officer, Business Performance Group	

Introduction

Council information is created or captured during the course of council business and forms a record of business transactions. It may have ongoing relevance to the person who created or captured it, and to others. Accordingly, it forms part of council's business record.

All information created, received or kept in the official capacity of a councillor is also part of council's business record.

An Information Asset Register will support this policy, identifying council's information and enabling access, use, re-use and management of information.

The Queensland Government Information Security Classification Framework (QGISCF) is used to ensure appropriate levels of systems and levels of control are implemented.

The Employee Code of Conduct requires that all council employees access only information and records required to perform official council duties, and that they comply with privacy requirements. The Councillor Code of Conduct provides appropriate information usage guidance for Councillors, and Council's Customer Service Charter stipulates customer responsibilities.

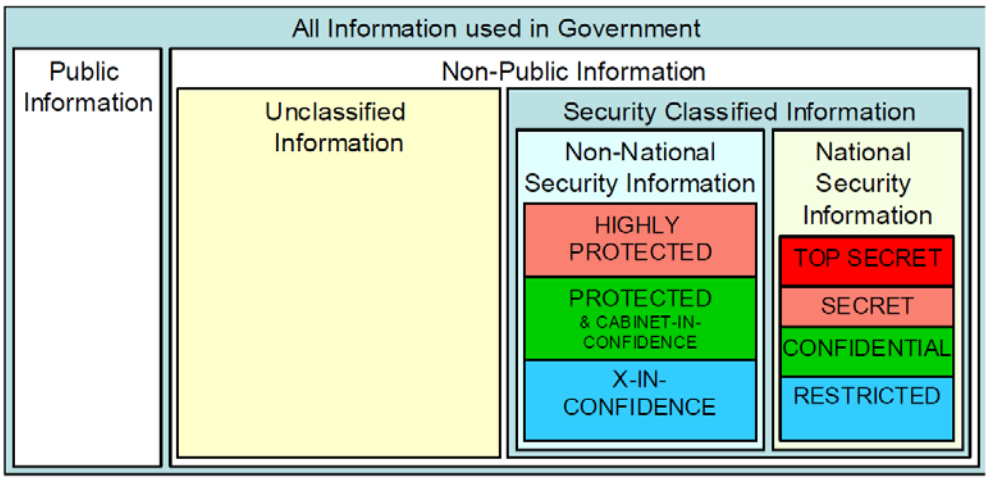
Providing appropriate access to information enhances decision-making, improves efficiency and reduces business risk.

Policy purpose

- Establish a Council Information Asset Register to assist with identification and management of council information, facilitate access and reuse, and minimise duplication of information.
- Establish that generally council information will be unclassified and therefore accessible across the organisation.
- Stipulate the specific instances when access to council information will be classified to protect confidentiality.
- Ensure appropriate governance of information access.
- Inform the development of council's Information Management Strategy.

Policy outcome

- Defined access to the non-public information used in council.
- Information access is monitored, reviewed and managed.
- Clear delegations of authority for the management of information.
- The Information Security Framework shown below is implemented in council business systems (note that council does not handle National Security Information).



- The classification of non-public information is consistent with the description; the actual classification process is based on a risk assessment defined in the framework, and applied in the information classification procedures in council.
- The classification of non-public information is consistent with the description; the actual classification process is based on a risk assessment defined in the framework, and applied in the information classification procedures in council.

Information Security Classification	*Description*
Highly Protected	Information assets that require a substantial degree of protection as compromise could cause serious damage to the State, the Government (including local government), commercial entities or members of the public. Very little belongs in the HIGHLY PROTECTED category and this is security classification level should be used sparingly. An example might be security measures and access information to some Airport facilities.
Protected	Information assets whose compromise could cause damage to the State, the Government, commercial entities or members of the public. This level of classification also includes Cabinet-in-Confidence which is similar to when council meets in closed session. As a principle, most security information assets will be adequately protected by the procedures given to X-IN-Confidence or Protected classifications.
X-in- Confidence	Information assets whose compromise could cause limited damage to the State, the Government, commercial entities or members of the public.
Unclassified	Information assets that have been assessed for security classification and do not require one of the classification levels. Information is marked with this classification to indicate that the assessment has been made. Information which has not been assessed is best marked Not-Yet-Security-Assessed and should be treated as Unclassified.

Policy scope

- Information in council business systems and repositories, network folders and hard-copy as defined in the information asset register.
- All councillors and council officers (permanent, maximum term, casual and full-time staff), contractors, agency casuals, and volunteers.
- Customers and members of the general public who access council information through the world wide web.

Policy statement

Council information underpins council efficiency, decision-making and risk management.

An Information Asset Register will facilitate access to and reuse of council information, and help minimise duplication.

The Queensland Government Information Security Classification Framework will be implemented in all council business systems.

Generally council information is unclassified and is accessible to all council officers.

For limited and specific categories of information, access will be restricted to particular employees to protect confidentiality. The Queensland Government Information Security Classification Framework will guide classification.

Classified information will be unclassified once conditions requiring classification no longer exist.

Access to secured information will be monitored, reviewed, reported and managed.

Annual review of the policy

The Chief Information Officer will conduct a review of this policy annually and will advise the results of that review, and make recommendations for change (if required or desirable) to the Strategic Knowledge Services Committee (SKSC).

Guiding principles

- Principles and directions issued by the CEO and /or the CEO's delegates under the relevant legislation determine the disclosure of information to the public (i.e. public information).
- The Employee Code of Conduct, Councillor Code of Conduct and Customer Service Charter specify appropriate use of council information

Roles and responsibilities

Position	Responsibilities
Chief Executive Officer	• Has responsibility for the keeping of proper records for the whole of council. • Is responsible under the *Local Government Act 2009* and other legislation include for management of resources (including information resources), keeping records, and ensuring their safe custody, and providing Council information to people entitled to access the information. The CEO has the power to give directions to staff on these matters. The CEO advances the principles of 'open government'. • Is responsible for determining the information security classification required to protect confidentiality.
Group Executives	• Ensure that their staff manage the information resources of the department in accordance with the directions and policies established by the CEO.
Branch Managers	• Implement information and knowledge management practices and systems that support business operations and maintain the information resources of their branch and that are consistent with this policy. • Ensure their staff develop their ability to use information systems and business records management practices and techniques.
Chief Information Officer	• Implements information management practices and systems that support the policies and directions of the CEO and Group Executives. • Provides reports on the performance of information management systems and the status of information resources. • Maintains register of information delegations.
Knowledge Solutions Manager	• Establishes and maintain council's Information Asset Register. • Advises on information security classifications. • Advises on directions, policies and systems that will ensure the proper keeping of correspondence, other records and information resources generally.
Nominated officers	• Recommend classification of information, identifying the legislative and risk factors that justify classification.

Position	Responsibilities
	• Advise on the access to be available to classified information. • Identify when classified information can be declassified.
Councillors and council officers	• Adhere to the relevant Code of Conduct governing appropriate use of information.
Customers and members of the public	• May access published information resources and request access to other information in ways defined by legislation. • Are required to treat our information resources when they use or access them or add to them in on-line transactions efficiently, effectively and ethically.

Measurement of success

- Improved business efficiency
- Improved information access across council and to the public
- Managed access to confidential information
- Clear delegations of authority for information management

Definitions

Information Assets Register: An information asset register listing the existing information assets across council. It enables users of information to identify the available information resources from a single source and provides information custodians with an overview of the information assets under their care.

Related policies and legislation

Local Government Act 2009: defines council responsibilities in managing information and records.

Knowledge Management Policy: improves the use of knowledge by individuals and groups in council and in the community

Business Recordkeeping Policy: directs and informs the creation, capture and use of council's business records

OTHER SUNSHINE COAST COUNCIL POLICIES AND GUIDELINES

Employee Code of Conduct

Councillor Code of Conduct

Customer Service Charter

CEO's Guideline May 2011

Complaints Management Process

Customer Request for Service and information Directed through a Councillor

Facebook Social Media Guidelines

Fraud & Corruption Policy

Information Technology Acceptable Use Policy

QUEENSLAND STATE GOVERNMENT LEGISLATION AND GUIDELINES

Local Government Act 2009

Right to Information Act 2009

Information Privacy Act 2009

Sustainable Planning Act 2009

Information Asset Register 2011

Public Sector Ethics Act 1994

Public Service Act 2008

Civil Liability Act 2003

Evidence Act 1977

Financial and Performance Management Standard 2009

POLICIES REPLACED BY THIS POLICY

Name	Policy owner	Type
Councillor Correspondence Public Records	Manager Council Services and Business Integration Finance and Business	To be confirmed
Confidential information - Caloundra	Knowledge Solutions Manager Finance and Business	Policy
Data custodianship operational guideline - Maroochy	Knowledge Solutions Manager & Spatial Information Manager Finance and Business	CMD
Information Management - Caloundra	Knowledge Solutions Manager Finance and Business	CMD

Version control:

Version	Reason/ Trigger	Change (Y/N)	Endorsed/ Reviewed by	Date
0.2	Draft for Consultation		Ron Robinson	*8/8/2012*
0.2.1	Version 0.2 reformatted	N		*8/8/2012*
2.2	Amended as directed by SKSC	Y	Ron Robinson	*7/9/2012*
2.3	Minor editing	N	Ron Robinson	*5/10/2012*
2.4	Updated as per new organisational structure		Corporate Governance	*05/02/2018*