

Organisational guideline

Information Access and Use Guideline

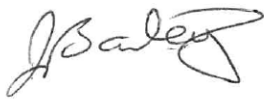
Approved by CEO:



11 Jan 2024

Related policy considered by ELT: 25 Oct 2023

GE advice date: 22 Dec 2023



Guideline purpose

The purpose of this guideline is to support and operationalise the Information Access and Use Policy which outlines Sunshine Coast Council's (Council) approach to the access, exchange, publishing, and classification of information.

Guideline scope

This guideline relates to information access, use and licensing, and applies to:

- All Council employees (including contingent workers, contractors, agency casuals, and volunteers).
- Partners, customers, and members of the general public who access Council information.

This guideline applies to all information created, collected, managed, and stored by Council in all forms including, but not limited to:

- Information in Council business systems and repositories, including information presented in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical forms.
- Data released for public access via Open Data Platform, Development.I and other public facing mediums.

The Employee Code of Conduct requires that all council employees only access information required to perform their role, and they comply with the Information Privacy Policy.

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

Guideline

Council is committed to the push model of providing public access to Council information to the maximum extent possible, unless there is a good reason not to, through the Information Access and Use Policy and Administrative Access and Right to Information Policy. The Information Sharing Procedure shows the steps required to approve the release of information that has a higher classification than PUBLIC.

Council datasets that have been classified as PUBLIC may be shared freely and can be published on the Council Open Data platform or Council website.

Open Data

The Open Data Procedure outlines the roles and responsibilities and steps to follow when publishing datasets to the Open Data portal.

Data sharing agreements

When sharing information with another government agency or community group and there is a requirement to control how the information is managed then a Data Sharing Agreement should be entered into.

Creative Commons Licencing

Creative Commons licences provide copyright owners with a range of free licences which facilitate the sharing and re-use of information. It is recommended to use the appropriate Creative Commons (CC) International licence which cover a wide range of copyright materials and licencing types. For further advice see the [Creative Commons Website](#)

Classification of Information Assets

Information collected, created, received, used, and shared by Council will be classified based on the Queensland Government Information Security Classification Framework (QGISCF). These security classification labels will govern how the Information Asset will be protected and managed.

Security controls are placed on information assets depending on their security classification and considering the three information security principles of Confidentiality, Integrity and Availability as shown below and in the Information Security Policy.

Element	Definition
Confidentiality	Risk of unauthorised/ inappropriate disclosure or release
Integrity	Risk to information quality
Availability	Risk to information not being available to authorised users

Classification Labels

The suitable release of information should be determined by the use of a Business Impact Level Assessment (BIL), using the Queensland Government Information Security Classification Framework (QGISCF). An example of a BIL can be found at *Appendix A*

Where the use of the BIL determines that there may be an impact to the confidentiality of the information asset the appropriate classification label should be applied to the information asset.

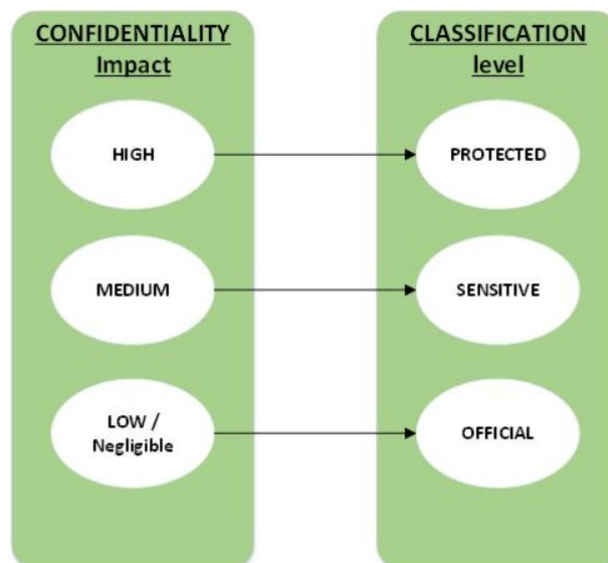
The confidentiality labels to be applied to classify Council’s information assets are:

Confidentiality requirement	Classification label	Minimum controls
Low	PUBLIC	As per QGEA and Council's risk assessment.
	OFFICIAL	As per QGEA and Council's risk assessment.
Medium	SENSITIVE	As per QGEA and Council's risk assessment.
High	PROTECTED	As per QGEA and Council's risk assessment. Council must consider the controls outlined for PROTECTED information in ACSM ISM.
National Security Information (NSI)		Not covered by QGISCF. Seek advice from QPS.

Figure 1: Confidentiality labels derived from the QGISCF.

Confidentiality business impact levels

The level of impact to an information asset through the loss of confidentiality defines the classification label that should be applied to that asset, according to the levels below.



Details of the classification labels

Classification label	Description
<p>PUBLIC (Nil or negligible confidentiality impact)</p>	<ul style="list-style-type: none"> • Authorised for unlimited public access. • Ready for publication via Open Data, Development.i, Council website etc. • May have Integrity or Availability requirements when controlled e.g., on a public website but should have nil Confidentiality requirements. <p>Examples of Public information may include, but are not limited to:</p> <ul style="list-style-type: none"> ▪ Media and press releases. ▪ Event schedules ▪ Non sensitive reports ▪ Research findings ▪ Council forms ▪ Council fees and charges schedules ▪ Ordinary meeting minutes ▪ Property boundary maps ▪ Road names
<p>OFFICIAL (Low confidentiality impact)</p>	<ul style="list-style-type: none"> • OFFICIAL represents most Council information by volume. • OFFICIAL information is routine information without special sensitivity or handling requirements. • All routine Council information is treated as OFFICIAL. Information classified as OFFICIAL should be available by default across Council. • Security measures should be proportionate and driven by the business requirement. <p>Examples of Official information may include, but are not limited to:</p> <ul style="list-style-type: none"> ▪ Internal meeting agendas ▪ Organisational charts ▪ Internal policies, procedures, and guidelines ▪ Working documents and drafts

Classification label	Description
<p>SENSITIVE</p> <p>(Moderate confidentiality impact)</p>	<ul style="list-style-type: none"> • The use of the SENSITIVE label indicates that information requires additional handling care due to its sensitivity or moderate business impact if compromised or lost. • SENSITIVE information must be stored in a system with the ability to control access e.g the eDRMS. <p>Examples of Sensitive information may include, but are not limited to:</p> <ul style="list-style-type: none"> ▪ Council business, whose compromise could affect Council's capacity to make decisions or operate, the public's confidence in Council, the stability of the economy and so on. ▪ Commercial interests, whose compromise could significantly affect the competitive process and provide the opportunity for unfair advantage. ▪ Legal professional privilege. ▪ Law enforcement operations whose compromise could adversely affect crime prevention strategies, particular investigations or adversely affect personal safety. ▪ Personal information, which is required to be safeguarded under the Information Privacy Act 2009 (QLD) ▪ Contracts with vendors (in probity stage) ▪ Employee records and personnel files
<p>PROTECTED</p> <p>(High confidentiality impact)</p>	<ul style="list-style-type: none"> • PROTECTED information requires the most careful safeguards due to its sensitivity or major business impact if compromised or lost. • PROTECTED information assets require a substantial degree of control as compromise could cause serious damage to the Council, commercial entities, or members of the public. • PROTECTED information must be stored in a system with the ability to control access e.g the eDRMS. <p>Examples of PROTECTED information may include, but are not limited to:</p> <ul style="list-style-type: none"> ▪ Name suppression registers ▪ Complaints and corruption investigations <p>There will be very few PROTECTED information assets at Council.</p>

	Public	Official	Sensitive	Protected
Storage	Can be stored on any device and on the internet. No restrictions on printing or copying the information, subject to copyright restrictions.	Information must be held within approved information systems as stated in the Acceptable Use Policy and Guidelines	Information must be held within approved information systems as stated in the Acceptable Use Policy and Guidelines. Paper records must not be left unattended and must be stored in a secure facility (i.e., Archives Centre).	Information must be held within approved information systems as stated in the Acceptable Use Policy and Guidelines. Paper records must not be left unattended and must be stored in a secure facility (i.e., Archives Centre)
Access	No restriction, information should always be publicly available ready.	All Official council information should be available for all council employees to access.	Information should be kept in systems with the ability to control access (i.e., eDRMS) to appropriate designated positions.	Information must be kept in systems with the ability to control access (i.e., eDRMS) to appropriate designated positions.
Transfer / Sharing	Information may be freely transmitted without restriction.	Information may be placed on the Council Intranet or other approved information system. Information can be internally shared via email or Teams. Information can be shared externally via email or “External Team” if deemed appropriate by Information Asset Custodian .	If transfer or sharing is required, then appropriate controls must be used to safeguard the information in line with the Information Security Policy. Branch Manager or above approval required to share Sensitive information externally.	If transfer or sharing is required, then appropriate controls must be used to safeguard the information in line with the ISMS. CEO approval required to share Protected information externally.

Principle

This guideline is supported by the Information Management principle of “Available” – Council information should be made available for use and re-use to the maximum extent possible.

Guideline application

This guideline is designed to support IS33 which is a foundational policy in the Queensland Government Enterprise Architecture and is considered best practice for Information Access and Use in Queensland.

Guideline review

The Chief Information Officer will oversee a review of this guideline in conjunction with the Information Access and Use Policy at least every 4 years, with policy risk factors to trigger earlier reviews as required.

Roles and Responsibilities

Role	Responsibility
Information Asset Owner	Is responsible under the <i>Local Government Act 2009</i> (Qld) for the safe custody of: <ul style="list-style-type: none"> • All records about the proceedings, accounts or transactions of Council or its committees. • All information owned or held by Council. The Information Asset Owner is the Chief Executive Officer (CEO).
Information Technology Steering Committee (ITSC)	Provides strategic advice to the Information Asset Owner on the management of Information Assets. Is an escalation point for advice on issues or risks related to information assets raised by Information Asset Custodians.
Chief Information Officer (CIO)	Responsible for overseeing regular reviews of this policy and advise results of the review and make recommendations for change (if required or desirable) to the ITSC.

<p>Information Asset Custodian</p>	<ul style="list-style-type: none"> • Recommending the appropriate security classification for information, identifying the legislative and risk factors that justify the classification. • Ensuring information assets are classified in accordance with the QGISCF and captured within Council’s IAR. • Advising on and approving the appropriate access and use of Council’s information assets based on the security classification. • Advising on and approving access controls for Council’s sensitive and protected information. • Identifying when the business impact for information has changed (e.g., local government meetings’ information considered sensitive or protected), leading to an updated classification level, resulting in information being made available more widely within Council or to the public. • Ensuring Council information is made available to the public to the maximum extent possible in accordance with legislative and policy requirements. • Ensuring the exchange of information with other government agencies and groups identified by Council is conducted in a secure way and in accordance with security classification levels, processes, guidelines, policy, and legislative requirements.
<p>Information Management Team Leader</p>	<ul style="list-style-type: none"> • Conducting monitoring activities across the IAR to ensure the management and maintenance of information assets within the register is compliant with relevant policies, procedures, regulations, and legislation. • Monitoring the regulatory environment to ensure any changes are accounted for and applied across Council’s policies, procedures, and guidelines. • Ensuring appropriate information management-related training is kept current and available for Council staff, including for Information Asset Custodians. • Providing high-level guidance to Council staff, including to Information Asset Custodians, about information management-related processes and procedures.

Measurements of success

Measure	Outcome sought
Right to Information requests	A decrease in formal access applications under the <i>Right to Information Act 2009</i> (Qld) and/or the <i>Information Privacy Act 2009</i> (Qld) relative to other release mechanisms
Open Data	Increase in the number of datasets available for public consumption on the Open Data Platform
Public Information Asset Register	Increase in the percentage of Information Assets listed on the Information Asset Register for public release
Information Security Classification	Improvement in the amount of council information classified against the QGISCF enabling appropriate security and access controls to be applied.

Definitions

Refer to any related Council policies for relevant definitions of common terms. The following contains definitions for terms specific to this guideline. For otherwise undefined terms, the plain English meaning informs interpretation.

Term	Definition
Information	Information is any collection of data that is processed, analysed, interpreted, organised, classified, or communicated in order to serve a useful purpose, present facts, or represent knowledge in any medium or form. This includes a presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical forms.
Information Asset	An identifiable collection of data stored in any manner and recognised as having value to enable the Council to perform its business functions, thereby satisfying a recognised Council requirement e.g., files, databases, paper-based and electronic documents, records, hardware items, software, or other infrastructure items.

Information Asset 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 Asset Custodians with an overview of the information assets under their care.
Information Asset Custodian	The recognised officer responsible for implementing and maintaining information assets according to the rules set by the owner to ensure proper quality, security, integrity, correctness, consistency, privacy, confidentiality, and accessibility.
Open Data	Initiatives by governments to make publicly funded, non-sensitive data available without restriction via the internet.
Open Data Platform	Council's website used for hosting Open Data sets and APIs

© Sunshine Coast Regional Council 2009-current

VERSION CONTROL				
Version	Reason/Trigger	Change	Endorsed/Reviewed by	Date
1.0	New guideline created	Guideline created	Team Leader Information Management	27/09/2023
1.1	Alignment to other policies and guidelines	Classification examples and advice on alignment to Information Security Policy added	Information Management team	02/11/2023
2.0	Final draft reviewed by Data Analytics team	Add reference to Open Data and External sharing procedures	Data Analytics Team Leader	22/11/2023
3.0	Corporate Governance review	No change	Coordinator Integrity Management	27/11/2023
4.0	GE Business Performance review		GE Business Performance	08/12/2023

GUIDELINE INFORMATION

Title	Information Access and Use Guideline	
Purpose	The purpose of this guideline is to support and operationalise the Information Access and Use Policy which outlines Sunshine Coast Council's (Council) approach to the access, exchange, publishing, and classification of information.	
Document number	D2023/1242904	
Corporate Plan reference	Goal	Our Outstanding Organisation
	Pathway	Maintain a sustainable organisation that is well placed to respond to the needs of our growing region.
	Service Output	Digital Information Services
GE advice date	22 December 2023	
CEO approval date	11 January 2024	
Effective date	11 January 2024	
Review schedule	A full review must be undertaken within every four years, and reviewed guideline document must be provided to highest level approval authority for endorsement. Reviews may occur more regularly as required, having regard to a policy risk assessment.	
Last review	Established 2023	
Next review	2026	
Guideline holder	The Manager responsible for this guideline is: Chief Information Officer (CIO)	
Approval authority	CIO has authority to approve material changes to keep guideline updates responsive to user need, CIO authority for future endorsement is recommended	

RELATED DOCUMENTS

Legislation	Local Government Act 2009 (QLD) Public Records Act (2002) QLD Right to Information Act 2009 (QLD) Information Privacy Act (2009) QLD
Policy setting documents	Queensland Government Enterprise Architecture Information Asset Custodianship Policy (IS33) Queensland Government Information Security Classification Framework (QGISCF) ISO 16175 (Information and documentation — Processes and functional requirements for software for managing records).
Operational documents	Information Access and Use Policy Open Data Guidelines Records Management Policy Information Security Policy Information Asset Custodianship Policy Administrative Access and Right to Information Policy

Appendix A Confidentiality – Business impact assessment - example

Confidentiality Impact		Low	Medium	High
Risk to Individual safety	Consider risk of injury or impact on safety, as well as the possibility of loss of life. An example could include release of names or locations of undercover officers, people under protection orders.	Potential risk to individual safety	Direct actual risk to individual safety	Direct actual risk to individual life / lives
Distress caused to any party	From the client's or public's point of view, distress could be caused by many things, including the release of personal information.	Some distress from information release	Significant and real distress	-
Damage to any party's standing or reputation.	Effect on any party's standing or reputation. Issues to consider include potential for adverse publicity, either locally or wider and the potential for damage occurring to either the service provider's or client's ongoing reputation.	Potential risk to reputation	Significant and long-lasting damage to reputation.	-
Inconvenience to any party	Releasing information which could lead to identity fraud being perpetrated.	Some inconvenience	Significant inconvenience, direct significant tangible loss	-
Public order	Whether release of information could pose a risk to community relations and public order.	Public order affected	Public order significantly affected	Complete loss of public order
Release of commercially sensitive data to third parties	Would disclosure of information have a commercial impact on any party, commercially sensitive information that could impact on current or future business.	Some commercial impact	Significant commercial impact	-
Release of personally sensitive data to third parties	Privacy - Would release violate legislative or regulatory guidelines such as information privacy principles?	Moderate privacy impact	Significant loss of sensitive personal information	-
Impact government finances, economic interests	Impact on council finances or economic and commercial interests - Would disclosure of information result in financial or economic consequences to council? E.g., Disclosure of planning results in changing property valuations.	Low - Moderate financial loss	Significant financial loss, loss of PCI: DSS	

Confidentiality Impact		Low	Medium	High
Financial loss to agency / service provider	Consider this from the service provider's perspective - what losses could they incur? Considerations include possibility of fraud, a party illegally transferring money, a party gaining control of assets they don't legally own (e.g., by using information to establish an identity which is not theirs).	Low - Moderate financial loss	Significant financial loss, possible organisational collapse	-
Threat or opportunity to council's systems or capacity to conduct their business	Would release of this information have the potential to prevent or reduce council or external party ability to conduct their business? For how long would this reduction/prevention last?	Low - Moderate threat to capacity	Significant threat to council systems or capacity to conduct business over years	-
Assistance to crime or impact on its detection	Would release of this information have the potential to assist in the conduct of a crime or terrorist activity?	Release of information may assist the conduct of a crime	Release of information provides moderate assistance to the conduct of a crime	Suspects of major crime escape justice
Impact on development or operation of council policy	Would disclosure cause negative or positive impact to council during the stages where policy is being formulated or implemented?	Policy development is slowed	Significant policy development is halted.	-
Impact on the environment	Impact the environment through information release.	Environmental impact	Catastrophic environmental impact	-
Impact on agency or Council workforce	Affect council ability to function.	Damage council ability to function	Significantly damage council ability to function over years	-
Impact on risk of litigation	Litigation against Sunshine Coast Council is increased.	Moderate	Significant risk of litigation	-
Impacts on National Infrastructure	Damage to Queensland critical infrastructure.	Damaging or disrupting infrastructure	Damaging or disrupting significant infrastructure	-
Confidentiality BIL	If there is deemed to be negligible or no confidentiality impact then (PUBLIC) can be used	Low (OFFICIAL or PUBLIC)	Medium (SENSITIVE)	High (PROTECTED)