



**ORANGE CITY COUNCIL
ORDINARY COUNCIL MEETING**

**ATTACHMENTS
COUNCIL ITEM 5.2
STRATEGIC POLICY REVIEWS**

15 NOVEMBER 2022

ATTACHMENT ITEMS

5.2 STRATEGIC POLICY REVIEWS

Attachment 1	Draft - ST04 - Councillor Access to Information and Interaction with Staff - For Exhibition	3
Attachment 2	Draft - ST05 - Councillor Records Management - For Exhibition	14
Attachment 3	Draft - ST13 - Cyber Security - For Exhibition	21



Strategic Policy – ST04

Councillor Access to Information and Interaction with Staff

FOR EXHIBITION

PO Box 35, Orange
NSW 2800 Australia

135 Byng Street, Orange
NSW 2800 Australia

P: +61 2 6393 8000
F: +61 2 6393 8199

council@orange.nsw.gov.au
www.orange.nsw.gov.au



All policies can be reviewed or revoked by a resolution of Council, at any time.

TABLE OF CONTENTS

POLICY OVERVIEW	3
1 INTRODUCTION	3
2 APPLICATION	4
3 POLICY OBJECTIVES.....	4
4 PRINCIPLES, ROLES AND RESPONSIBILITIES.....	4
5 THE COUNCILLOR REQUESTS SYSTEM	6
6 ACCESS TO COUNCIL STAFF	8
7 COUNCILLOR ACCESS TO COUNCIL BUILDINGS	9
8 APPROPRIATE AND INAPPROPRIATE INTERACTIONS	9
9 COMPLAINTS.....	10
SCHEDULE 1 – AUTHORISED STAFF CONTACTS FOR COUNCILLORS.....	10
SCHEDULE 2 – WORKFLOW FOR COUNCILLOR REQUEST SYSTEM	11



All policies can be reviewed or revoked by a resolution of Council, at any time.

POLICY OVERVIEW

Purpose

The purpose of this policy is to outline compliance with the Local Government Act 1993 and the Government Information (Public Access) Act 2009, and that Councillors have the same information upon which to make decisions and to ensure that any interaction between Councillors and staff is consistent with Council's Code of Conduct.

This policy :

- documents communication channels to ensure the provision of accurate information from Council records systems to Councillors, within reasonable timeframes to assist Councillors in the performance of their civic duty
- defines appropriate professional interactions between Councillors and Council staff
- outlines Councillors' rights of access to Council buildings
- identifies inappropriate interactions between Councillors and Council staff
- outlines a process for reporting breaches.

Applicability

This policy applies to all Councillors when requesting information and to staff when providing information.

The Code of Conduct overrides this policy to the extent of information provided to the Conduct Review Panel or Conduct Reviewer.

Scope

Schedule 1 of the Government Information (Public Access) Regulation 2009 provides that certain documents held by Council are to be made publicly available for inspection, free of charge. This policy supports that requirement and outlines the procedure for accessing such information.

Interactions between Councillors and staff at Council meetings are regulated by Council's Code of Meeting Practice (Local Government

(General) Regulation 2005 [Part 10 – Meetings] and Council's Code of Conduct.

Clause 3.1(b) of the Model Code of Conduct provides that council officials must not conduct themselves in a manner that is contrary to a council's policies. If adopted by a council, a breach of the policy may also constitute a breach of council's code of conduct.

Concerns or complaints about the administration of a council's councillor request system should be raised with the Chief Executive Officer (or the Mayor in the case of a complaint about the Chief Executive Officer). If the matter cannot be resolved locally, councillors may raise their concerns with OLG.

1 INTRODUCTION

1.1. The Councillor and Staff Interaction Policy (the Policy) provides a framework for councillors when exercising their civic functions by specifically addressing their ability to interact with, and receive advice from, authorised staff.

1.2. The Policy complements and should be read in conjunction with Council's Code of Conduct.

1.3. The aim of the Policy is to facilitate a positive working relationship between councillors, as the community's elected representatives, and staff, who are employed to administer the operations of the Council. The Policy provides direction on interactions between councillors and staff to assist both parties in carrying out their day-to-day duties professionally, ethically and respectfully.

1.4. It is important to have an effective working relationship that recognises the important but differing contribution both parties bring to their complementary roles.



All policies can be reviewed or revoked by a resolution of Council, at any time.

2 APPLICATION

- 2.1. This Policy applies to all Councillors and Council Staff.
- 2.2. This Policy applies to all interactions between Councillors and staff, whether face-to-face, online (including social media and virtual meeting platforms), by phone, text message or in writing.
- 2.3. This Policy applies whenever interactions between Councillors and staff occur, including inside or outside of work hours, and at both council and non-council venues and events.
- 2.4. This Policy does not confer any delegated authority upon any person. All delegations to staff are made by the Chief Executive Officer.
- 2.5. The Code of Conduct provides that council officials must not conduct themselves in a manner that is contrary to the Council's policies. A breach of this Policy will be a breach of the Code of Conduct.

3 POLICY OBJECTIVES

- 3.1. This Policy applies to all councillors and council staff.
- 3.2. This Policy applies to all interactions between councillors and staff, whether face-to-face, online (including social media and virtual meeting platforms), by phone, text message or in writing.
- 3.3. This Policy applies whenever interactions between councillors and staff occur, including inside or outside of work hours, and at both council and non-council venues and events.
- 3.4. This Policy does not confer any delegated authority upon any person. All delegations to staff are made by the Chief Executive Officer.
- 3.5. The Code of Conduct provides that council officials must not conduct themselves in a manner that is contrary to the Council's policies. A breach of this Policy will be a breach of the Code of Conduct.

4 PRINCIPLES, ROLES AND RESPONSIBILITIES

- 4.1. Several factors contribute to a good relationship between councillors and staff. These include goodwill, understanding of roles, communication, protocols, and a good understanding of legislative requirements.
- 4.2. The Council's governing body and its administration (being staff within the organisation) must have a clear and sophisticated understanding of their different roles, and the fact that these operate within a hierarchy. The administration is accountable to the Chief Executive Officer, who in turn, is accountable to the Council's governing body.
- 4.3. Section 232 of the Local Government Act 1993 (the LGA) states that the role of a councillor is as follows:
 - a) to be an active and contributing member of the governing body
 - b) to make considered and well-informed decisions as a member of the governing body
 - c) to participate in the development of the integrated planning and reporting framework
 - d) to represent the collective interests of residents, ratepayers and the local community
 - e) to facilitate communication between the local community and the governing body
 - f) to uphold and represent accurately the policies and decisions of the governing body
 - g) to make all reasonable efforts to acquire and maintain the skills necessary to perform the role of a councillor.
- 4.4. The administration's role is to advise the governing body, implement Council's decisions and to oversee service delivery.



All policies can be reviewed or revoked by a resolution of Council, at any time.

4.5. It is beneficial if the administration recognises the complex political environments in which elected members operate and acknowledge that they work within a system that is based on democratic governance. Councillors similarly need to understand that it is a highly complex task to prepare information and provide quality advice on the very wide range of issues that Council operations cover.

4.6. Council commits to the following principles to guide interactions between councillors and staff:

Principle

Achieved by

Equitable and consistent

Ensuring appropriate, consistent and equitable access to information for all councillors within established service levels

Considerate and respectful

Councillors and staff working supportively together in the interests of the whole community, based on mutual respect and consideration of their respective positions

Ethical, open and transparent

Ensuring that interactions between councillors and staff are ethical, open, transparent, honest and display the highest standards of professional conduct

Fit for purpose

Ensuring that the provision of equipment and information to councillors is done in a way that is suitable, practical and of an appropriate size, scale and cost for a client group of twelve (12) people.

Accountable and measurable

Providing support to councillors in the performance of their role in a way that can be measured, reviewed and improved based on qualitative and quantitative data

4.7. Councillors are members of the Council's governing body, which is responsible for directing and controlling the affairs of the Council in accordance with the LGA. Councillors need to accept that:

- a) responses to requests for information from councillors may take time and consultation to prepare and be approved prior to responding
- b) staff are not accountable to them individually
- c) they must not direct staff except by giving appropriate direction to the Chief Executive Officer by way of a council or committee resolution, or

by the mayor exercising their functions under section 226 of the LGA

- d) they must not, in any public or private forum, direct or influence, or attempt to direct or influence, a member of staff in the exercise of their functions
- e) they must not contact a member of staff on council-related business unless in accordance with this Policy
- f) they must not use their position to attempt to receive favourable treatment for themselves or others.



All policies can be reviewed or revoked by a resolution of Council, at any time.

4.8. The Chief Executive Officer is responsible for the efficient and effective day-to-day operation of the Council and for ensuring that the lawful decisions of the Council are implemented without undue delay. Council staff need to understand:

- a) they are not accountable to individual councillors and do not take direction from them. They are accountable to the Chief Executive Officer, who is in turn accountable to the Council's governing body
- b) they should not provide advice to councillors unless it has been approved by the Chief Executive Officer or a staff member with a delegation to approve advice to councillors
- c) they must carry out reasonable and lawful directions given by any person having the authority to give such directions in an efficient and effective manner
- d) they must ensure that participation in political activities outside the service of the Council does not interfere with the performance of their official duties
- e) they must provide full and timely information to councillors sufficient to enable them to exercise their civic functions in accordance with this Policy.

5 THE COUNCILLOR REQUESTS SYSTEM

5.1. Councillors have a right to request information provided it is relevant to councillor's exercise of their civic functions. This right does not extend to matters about which a Councillor is merely curious.

5.2. Councillors do not have a right to request information about matters that they are prevented from participating in decision-making on because of a conflict of interest, unless the information is otherwise publicly available.

5.3. The Chief Executive Officer may identify Council support staff (the Councillor Support Officer) under this Policy for the management of requests from Councillors.

5.4. Councillors can use the Councillor requests system to:

- a) request information or ask questions that relate to the strategic position, performance or operation of the Council
- b) bring concerns that have been raised by members of the public to the attention of staff
- c) request ICT or other support from the Council administration
- d) request that a staff member be present at a meeting (other than a meeting of the council) for the purpose of providing advice to the meeting.

5.5. Councillors must, to the best of their knowledge, be specific about what information they are requesting, and make their requests respectfully. Where a councillor's request lacks specificity, the Chief Executive Officer or staff member authorised to manage the matter is entitled to ask the councillor to clarify their request and the reason(s) why they are seeking the information.



All policies can be reviewed or revoked by a resolution of Council, at any time.

- 5.6. Staff must make every reasonable effort to assist councillors with their requests and do so in a respectful manner.
- 5.7. Schedule 2 to this Policy sets out the process for the Management of Councillor requests:
- Requests on behalf of residents will be directed through Council's Customer Request Management System in the first instance.
 - Requests, other than initial customer requests, which do not require the expenditure of funds or redirection of resources will be managed through the Councillor request system. The Chief Executive Officer or the staff member authorised to manage a Councillor request will provide an acknowledgement within **two (2) business days** and a further, if not final response within **ten (10) business days**.
 - Where a response cannot be provided within that timeframe, the councillor will be advised, and the information will be provided as soon as practicable.
 - Requests requiring the expenditure of funds or redirection of resources are to be made by way of a Notice of Motion in accordance with Council's adopted Code of Meeting Practice.
 - Responses to Councillor requests will be made available to all Councillors. This is in accordance with the Code of Conduct which provides that members of staff who provide information to a particular Councillor in the performance of their official functions must also make it available to any other Councillor who requests it and in accordance with Council procedures.
- 5.8. Requests under clause 5.4(d) must be made **5 business days** before the meeting. The Chief Executive Officer, or members of staff that are listed at Schedule 1 of this Policy, are responsible for determining:
- whether a staff member can attend the meeting; and
 - which staff member will attend the meeting.
- Staff members who attend such meetings must be appropriately senior and be subject matter experts on the issues to be discussed at the meeting.
- 5.9. Councillors are required to treat all information provided by staff appropriately and to observe any confidentiality requirements.
- 5.10. Staff will inform councillors of any confidentiality requirements for information they provide so councillors can handle the information appropriately.
- 5.11. Where a councillor is unsure of confidentiality requirements, they should contact the Chief Executive Officer, or the staff member authorised to manage their request.
- 5.12. The Chief Executive Officer may refuse access to information requested by a councillor if:
- the information is not necessary for the performance of the councillor's civic functions, or
 - if responding to the request would, in the Chief Executive Officer's opinion, result in an unreasonable diversion of staff time and resources, or
 - the councillor has previously declared a conflict of interest in the matter and removed themselves from decision-making on it, or
 - the Chief Executive Officer is prevented by law from disclosing the information.



All policies can be reviewed or revoked by a resolution of Council, at any time.

- 5.13. Where the Chief Executive Officer refuses to provide information requested by a councillor, they must act reasonably. The Chief Executive Officer must advise a councillor in writing of their reasons for refusing access to the information requested.
- 5.14. Where a Councillor's request for information is refused by the Chief Executive Officer on the grounds referred to under clause 5.12 (a) or (b), the councillor may instead request the information through a resolution of the council by way of a notice of motion. This clause does not apply where the Chief Executive Officer refuses a councillor's request for information under clause 5.12 (c) or (d).
- 5.15. Nothing in clauses 5.12, 5.13, and 5.14 prevents a councillor from requesting the information in accordance with the Government Information (Public Access) Act 2009.
- 5.16. Where a councillor persistently makes requests for information which, in the Chief Executive Officer's opinion, result in a significant and unreasonable diversion of staff time and resources the council may, on the advice of the Chief Executive Officer, resolve to limit the number of requests the councillor may make.
- 5.17. Councillor requests are state records and must be managed in accordance with the State Records Act 1998.
- 5.18. A report will be provided to Council **every 6 months** regarding the performance and efficiency of the Councillor requests system against established key performance indicators.
- 6.2. Councillors can contact staff listed in Schedule 1 about matters that relate to the staff member's area of responsibility.
- 6.3. Councillors should as far as practicable, only contact staff during normal business hours.
- 6.4. If councillors would like to contact a member of staff not listed in Schedule 1, they must receive permission from the Chief Executive Officer.
- 6.5. If a councillor is unsure which authorised staff member can help with their enquiry, they can contact the Chief Executive Officer or the Councillor Support Officer who will provide advice about which authorised staff member to contact.
- 6.6. The Chief Executive Officer or a member of the Council's executive leadership team may direct any staff member to contact councillors to provide specific information or clarification relating to a specific matter.
- 6.7. A councillor or member of staff must not take advantage of their official position to improperly influence other councillors or members of staff in the performance of their civic or professional duties for the purposes of securing a private benefit for themselves or for another person. Such conduct should be immediately reported to the Chief Executive Officer or Mayor in the first instance, or alternatively to the Office of Local Government, NSW Ombudsman, or the NSW Independent Commission Against Corruption.

6 ACCESS TO COUNCIL STAFF

- 6.1. Councillors may directly contact members of staff that are listed in Schedule 1 of this Policy. The Chief Executive Officer may amend this list at any time and will advise councillors promptly of any changes.



All policies can be reviewed or revoked by a resolution of Council, at any time.

7 COUNCILLOR ACCESS TO COUNCIL BUILDINGS

- 7.1. Councillors are entitled to have access to the council chamber, committee room, mayor's office (subject to availability), councillors' rooms, and public areas of Council's buildings during normal business hours for meetings. Councillors needing access to these facilities at other times must obtain approval from the Chief Executive Officer.
- 7.2. Councillors must not enter staff-only areas of Council buildings without the approval of the Chief Executive Officer.

8 APPROPRIATE AND INAPPROPRIATE INTERACTIONS

- 8.1. Examples of appropriate interactions between councillors and staff include, but are not limited to, the following:

- a) councillors and council staff are courteous and display a positive and professional attitude towards one another
- b) council staff ensure that information necessary for councillors to exercise their civic functions is made equally available to all councillors, in accordance with this Policy and any other relevant Council policies
- c) council staff record the advice they give to councillors in the same way they would if it was provided to members of the public
- d) council staff, including Council's executive team members, document councillor requests via the councillor requests system
- e) council meetings and councillor briefings are used to establish positive working relationships and help councillors to gain an understanding of the complex issues related to their civic duties

- f) councillors and council staff feel supported when seeking and providing clarification about council related business

- g) councillors forward requests through the councillor requests system and staff respond in accordance with the timeframes stipulated in this Policy

- 8.2. Examples of inappropriate interactions between councillors and staff include, but are not limited to, the following:

- a) councillors and council staff conducting themselves in a manner which:
 - i. is contrary to their duties under the Work Health and Safety Act 2011 and their responsibilities under any policies or procedures adopted by the Council to ensure workplace health and safety
 - ii. constitutes harassment and/or bullying within the meaning of the Code of Conduct, or is unlawfully discriminatory
- b) councillors approaching staff and staff organisations to discuss individual or operational staff matters (other than matters relating to broader workforce policy such as, but not limited to, organisational restructures or outsourcing decisions), grievances, workplace investigations and disciplinary matters
- c) staff approaching councillors to discuss individual or operational staff matters (other than matters relating to broader workforce policy such as, but not limited to, organisational restructures or outsourcing decisions), grievances, workplace investigations and disciplinary matters
- d) subject to clause 5.12, staff refusing to give information that is available to other councillors to a particular councillor



All policies can be reviewed or revoked by a resolution of Council, at any time.

- e) councillors who have lodged an application with the council, discussing the matter with staff in staff-only areas of the council
- f) councillors being overbearing or threatening to staff
- g) staff being overbearing or threatening to councillors
- h) councillors making personal attacks on staff or engaging in conduct towards staff that would be contrary to the general conduct provisions in Part 3 of the Code of Conduct in public forums including social media
- i) councillors directing or pressuring staff in the performance of their work, or recommendations they should make
- j) staff providing ad hoc advice to councillors without recording or documenting the interaction as they would if the advice was provided to a member of the community

8.3. Where a councillor engages in conduct that, in the opinion of the Chief Executive Officer, puts the health, safety or welfare of staff at risk, the Chief Executive Officer may restrict the councillor's access to staff.

8.4. Any concerns relating to the conduct of staff under this Policy should be raised with the Chief Executive Officer.

9 COMPLAINTS

9.1. Complaints about a breach of this policy should be made to the Chief Executive Officer (if the complaint is about a Councillor or member of Council staff), or the Mayor (if the complaint is about the Chief Executive Officer).

9.2. Clause 9.1 does not operate to prevent matters being reported to OLG, the NSW Ombudsman, the NSW Independent Commission Against Corruption or any other external agency.

SCHEDULE 1 – AUTHORISED STAFF CONTACTS FOR COUNCILLORS

1. Clause 6.1 of this Policy provides that councillors may directly contact members of staff that are listed below. The Chief Executive Officer may amend this list at any time.
2. Councillors can contact staff listed below about matters that relate to the staff member's area of responsibility.
3. Councillors should as far as practicable, only contact staff during normal business hours.
4. If councillors would like to contact a member of staff not listed below, they must receive permission from the Chief Executive Officer or their delegate.
5. If a councillor is unsure which authorised staff member can help with their enquiry, they can contact the Chief Executive Officer or the Councillor Support Officer who will provide advice about which authorised staff member to contact.
6. In some instances, the Chief Executive Officer or a member of the Council's executive leadership team may direct a council staff member to contact councillors to provide specific information or clarification relating to a specific matter.

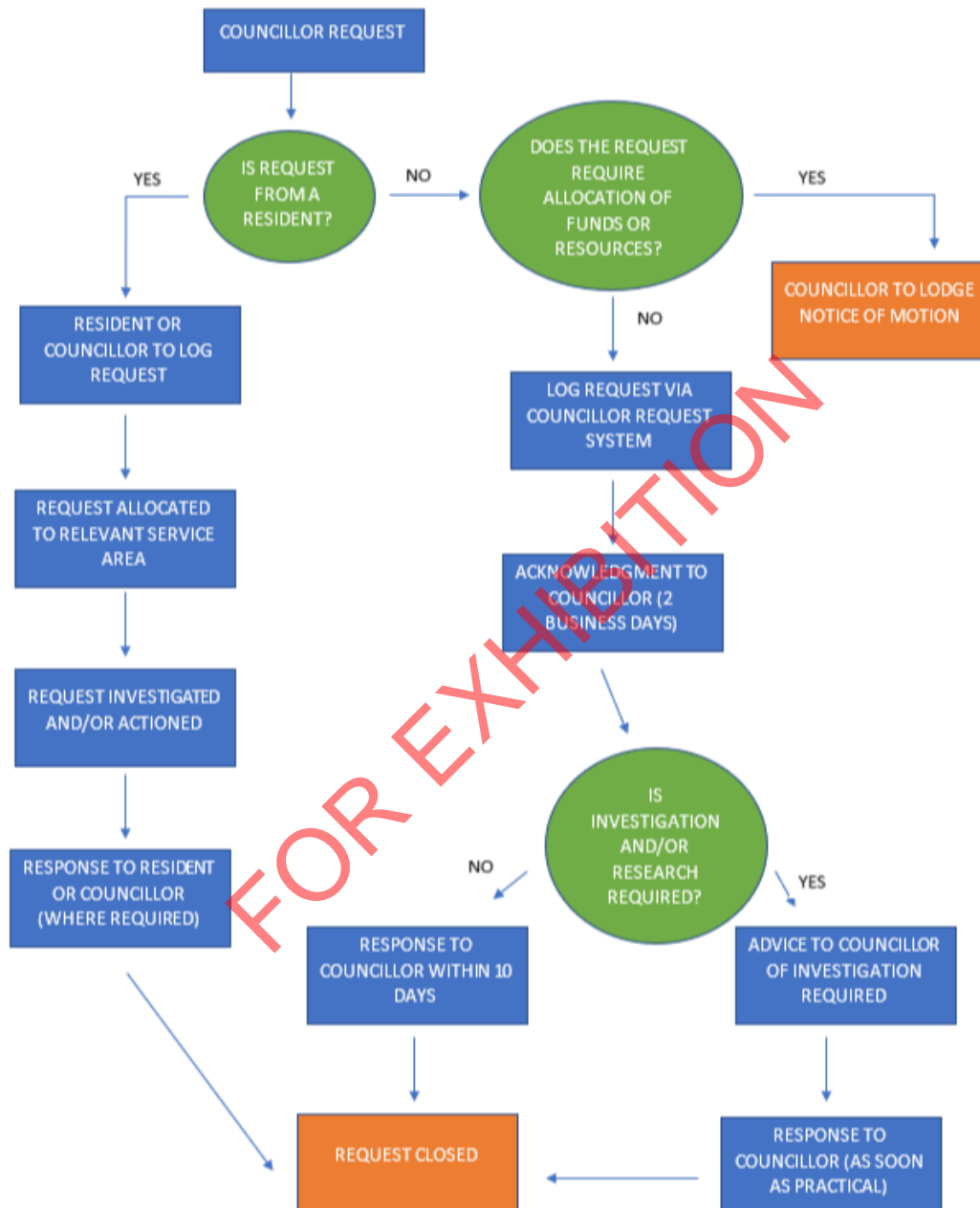
Authorised Staff Members

- Chief Executive Officer
- Director Corporate & Commercial Services
- Director Community, Recreation & Cultural Services
- Director Technical Services
- Director Development Services
- Chief Financial Officer
- Executive Support Manager
- Executive Support Officer
- Manager Communications & Engagement



All policies can be reviewed or revoked by a resolution of Council, at any time.

SCHEDULE 2 – WORKFLOW FOR COUNCILLOR REQUEST SYSTEM



ST04 – Strategic Policy – Councillor Access to Information and Interaction with Staff

Review Due: November 2024

Version 1_22

Last Revision: 2 April 2019

Approved by:

Minute Number:

Approval Date:



Strategic Policy ST05

Councillor Records Management

FOR EXHIBITION

PO Box 35, Orange
NSW 2800 Australia

135 Byng Street, Orange
NSW 2800 Australia

P: +61 2 6393 8000
F: +61 2 6393 8199

council@orange.nsw.gov.au
www.orange.nsw.gov.au



All policies can be reviewed or revoked by a resolution of Council, at any time.

TABLE OF CONTENTS

1	OVERVIEW	3
2	INTRODUCTION	3
3	CREATING AND CAPTURING RECORDS	4
4	UNAUTHORISED ACCESS OR DISCLOSURE OF COUNCIL RECORDS.....	6
5	HANDLING AND STORAGE OF RECORDS.....	6
6	DISPOSAL OF RECORDS	6
7	ACCESS TO RECORDS.....	7
8	SECURITY AND CONFIDENTIALITY OF RECORDS	7
9	ACCESS TO RECORDS.....	7
10	REFERENCES	7

FOR EXHIBITION



All policies can be reviewed or revoked by a resolution of Council, at any time.

1 OVERVIEW

Purpose

- 1.1 Council is bound by the State Records Act 1998 and the Government Information (Public Access) Act 2009 which establish rules for record keeping to ensure transparency and accountability. Councillors, in undertaking their role as an elected member, are subject to these rules and must ensure proper records management, as set out in this Policy and associated Procedure.
- 1.2 To ensure that full and accurate records of the activities and decisions of Councillors, in the course of their official duties for Council are created, managed and disposed of in accordance with Council's organisational needs, the State Records Act 1998 and the Government Information (Public Access) Act 2009, the Councillor Records Management Policy has been created.
- 1.3 A Council is identified as a public office under section 3(1) of the Act. Councillors are subject to the Act when they create or receive 'Records' while undertaking business on Council's behalf. They are not subject to the Act when conducting personal business or business that is unrelated to their role as Councillors.

Applicability

- 1.4 All Councillors must comply with this Policy in their conduct of official business for Council. Official business includes business relevant to the performance of the function and duties of the Councillor. This Policy applies to records in all formats, including electronic records.

Procedure

- 1.5 Council has adopted the "Model Records Management for Councillors" procedure prescribed by Records NSW. This procedure is to be applied when dealing with Council records. Councillors should be aware that any document of information held, created or received relating to Council business, falls within the definition of "Government Information" under the Government Information (Public Access) Act 2009.
- 1.6 Any correspondence directed to Councillors via Orange City Council will be opened by Records Staff and processed in accordance with this policy.

2 INTRODUCTION

What is a Record?

- 2.1 A "Record" is 'any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means' (State Records Act 1998, Section 3(1))
- 2.2 A "State Record" is 'any record made and kept or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public office, or for the use of a public office' (State Records Act 1998, Section 3(1)).

Examples of State Records

- 2.3 Examples of "State Records" include (but are not limited to):
 - Correspondence, including emails, relating to any Council business (including correspondence sent to a Council-provided or private email or postal address)
 - A petition received from a community group
 - Declarations concerning a Councillor's pecuniary interests
 - Speech notes made for addresses given at official Council events



All policies can be reviewed or revoked by a resolution of Council, at any time.

- Complaints, suggestions or enquiries by residents about Council services
- Any written response provided by the Councillor to any of the above examples.

Examples that are NOT State Records

2.4 Records which are created, sent or received by Councillors when they are not discharging functions of Council are not considered to be State records for the purposes of the State Records Act 1998.

Examples of records that are not State records include (but are limited to):

- Records relating to political or electoral issues eg lobbying for votes, supportive emails from members of the community regarding elections or political stances
- Communications regarding matters of personal/general interest rather than Council interest eg information from environmental or other interest groups not specific to issues being considered by Councillors or Council
- Records relating to attendance at sports functions, church fetes, community functions when the Councillor is not representing Council
- Personal records of Councillors such as personal emails, character references for friends (these should not be written on Council letterhead or via Council email), nomination for awards, and letters to local newspapers etc that are not related to Council business.

Importance of Record Keeping

2.5 Accurate record keeping provides protection for Councillors, in the event that questions are raised regarding conduct. Documenting events, activities and decisions enables Councillors to recall or provide information on a matter when required and supports transparency of Councillor Conduct.

2.6 Records are a vital asset to Council. Many records created and received by Councillors have the potential to:

- Support the work of Councillors and Council's Delivery/Operational Plan, management and administration.
- Help Councillors and Council deliver customer service in an efficient fair and equitable manner.
- Provide evidence of Councillor's actions and decisions and establish precedents for future decision making.
- Protect the rights and interests of the Council, Councillors and customers.

3 CREATING AND CAPTURING RECORDS

What records to create and capture

3.1 Councillors should create and capture full and accurate records of any significant business undertaken in the course of their official duties for Council. Significant business can include:

- Providing advice, instructions or recommendations
- Drafts of documents for Council containing significant annotations or submitted for comment or approval by others
- Correspondence received and sent relating to their work undertaken for Council.

3.2 Council is responsible for:

- Creating and capturing records of Council or committee meetings
- Capturing any Records it sends to Councillors regarding Council business.

How to create records

3.3 Council has paper and electronic templates available for Councillors to create emails, letters and memos while conducting business for the Council. These will assist Councillors in ensuring that the essential information is recorded.



All policies can be reviewed or revoked by a resolution of Council, at any time.

- 3.4 Details of significant advice, commitments etc made during telephone or verbal conversations or via SMS should be recorded using the Council's standard meeting note template. Details should be recorded to include the following:

- Date and time
- Parties involved
- Summary of discussion
- Commitments
- Advice given
- Reasons for commitment/advice given

Note: Entries in Councillors' diaries are generally not adequate where there are recordkeeping requirements, they should be converted into a formal file note. These records should be made as soon as possible after the event to ensure the information is accurate.

How to capture records

- 3.5 Records of Council business that are created or received by Councillors (with the exception of those sent from Council as they are already captured) should be saved into official Council recordkeeping systems as soon as is practicable so that Council can assist with their long term management.

Paper records

- 3.6 Councillors are to keep paper records together and **at the end of each month**, transfer them to the Executive Support Office. Any confidential documents should be marked "CONFIDENTIAL" so that appropriate security measures can be implemented.

- 3.7 Records received from Councillors will be registered into Council's electronic document management system, with appropriate security controls attached.

Email/electronic records

- 3.8 Councillors are to provide any electronic records including emails, keeping such records together and **at the end of each month**, transfer them to the Executive

Support Office for registration into Council's Records System. Any confidential documents should be marked "CONFIDENTIAL" so that appropriate security measures can be implemented.

- 3.9 **For Councillors utilising a Council email address, a copy of all emails are automatically and securely stored in Council's archives.**

- 3.10 Records received from Councillors will be registered into Council's electronic document management system, with appropriate security controls attached in accordance with Council's Operational Policy – Records Management.

Councillor copies

- 3.11 Councillors may wish to retain a copy of any record. Copies should only be retained while needed for current Council business.

Councillor mail

- 3.12 Any incoming mail or email addressed to Councillors will be opened and processed by Records Staff. Mail or emails relating to Council business will be processed into Council's Electronic Document Management System where correspondence addressed to Councillors relates to operational matters, the letter will be referred to the Executive Support Office for forwarding to the relevant staff member for response. Councillors will be notified of this and be provided a copy of the correspondence. Any mail not related to Council business will be forwarded to the Councillor.

Creation of state records

- Should a Councillor create a document on behalf of Council that provides instructions, gives permission or consent, makes decisions, commitments or agreements binding on Council, then the document must be approved by the Mayor and/or Chief Executive Officer prior to it being sent. This applies to hard copy and electronic documents.



All policies can be reviewed or revoked by a resolution of Council, at any time.

Approval is not required for documents created purely on behalf of the Councillor, with no implicit or explicit impact on Orange City Council.

- 3.13 If it is deemed that a proposed document will contravene Council policy, breach a Council resolution or intention, the Mayor may rule the document inappropriate and require the document to be destroyed.

4 UNAUTHORISED ACCESS OR DISCLOSURE OF COUNCIL RECORDS

- 4.1 The Local Government Act 1993 section 664(1) prohibits the disclosure of information obtained in connection with the administration or execution of the Act, except in certain specific circumstances.

- 4.2 Councillors are also bound by the Council's Code of Conduct and Code of Meeting Practice **not** to:

- Attempt to access records they are not authorised to see
- Provide unauthorised access to other parties while Council records are in their care
- Disclose confidential information about Council business, or
- Disclose personal information of employees, clients etc without the subject's consent.

- 4.3 These rules help to ensure that Council and its staff and clients are protected and that the requirements of relevant legislation, such as privacy legislation, are met.

5 HANDLING AND STORAGE OF RECORDS

Damage or neglect of Records is an offence

- 5.1 Damage or neglect of a State Record is an offence under section 21 of the State Records Act.

Storing of records

- 5.2 When storing Council records temporarily the following rules apply:
- Records are to be kept away from known risks such as water, fire, mould,

vermin, vandalism, chemicals, direct sunlight, extreme temperatures etc

- Electronic records should be protected against additional hazards such as viruses
- Records should be secured appropriate to their level of sensitivity. No Council records should be left in plain view in vehicles or lying around the house.
- Councillors who are storing records of a sensitive or confidential nature should ensure that they are appropriately protected.

- 5.3 Copies of confidential business papers or documents can be returned to the Executive Support Office for destruction.

6 DISPOSAL OF RECORDS

Disposal in accordance with the State Records Act

- 6.1 State records held by Councillors must be disposed of in accordance with the State Records Act 1998. Such records should be returned to the Executive Support Office.

- 6.2 State Records NSW has issued General Retention and Disposal Authority – Local Government Records (GA39), which outlines classes of records and how long they should be kept before being legally destroyed or transferred to archives. Periods specified are based on relevant legislation, guidelines and standards. Failure to keep records for the length of time specified in the GA39 may put Councillors and Council at risk.

Liaison with Council for disposal

- 6.3 Councillors should liaise with the Manager Corporate Governance regarding the disposal of any records of Council business as Council is responsible for:

- Ensuring legislative requirements are met
- Ensuring destruction is undertaken appropriately (eg that no sensitive information is released due to inappropriate destruction methods), and



All policies can be reviewed or revoked by a resolution of Council, at any time.

- Documenting disposal decisions for accountability purposes.

7 ACCESS TO RECORDS

For information regarding Councillors' Access to Information/records, please refer to separate policy and associated procedure – Strategic Policy ST04 "Councillors Access to Information and Interaction with Staff".

8 SECURITY AND CONFIDENTIALITY OF RECORDS

Building controls

- 8.1 Council's paper records are kept securely in Council's buildings with security controls to protect against unauthorised access.

System controls

- 8.2 Council's records management software which controls electronic records restricts access according to security levels. Each electronic record is classified on registration and this classification determines users who have access to the record.

9 ACCESS TO RECORDS

Breaches of this Policy will be dealt with by the Mayor and/or Chief Executive Officer in accordance with the Code of Conduct.

10 REFERENCES

State Records Act

<https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-017#pt.1>

State Records - *What have records got to do with me?* available at:

<https://www.records.nsw.gov.au/recordkeeping/what-have-records-got-to-do-me-local-government>

State Records – *Recordkeeping Fundamentals for Councillors*, available at:

<https://www.records.nsw.gov.au/sites/default/files/Recordkeeping/Councillors%202018%20printable.pdf>

State Records - *Destruction of records*, available at:

<http://www.records.nsw.gov.au/recordkeeping/advice/retention-and-disposal/destruction-of-records>

State Records - *General retention and disposal authority: local government records* (GA39) available at:

<https://www.records.nsw.gov.au/recordkeeping/rules/gdas/ga39>

ST05 – Strategic Policy – Councillor Records Management

Review Due: November 2024	Version 1_22	Last Revision: 6 February 2018
Approved By:	Minute Number:	Approval Date:



Strategic Policy – ST13

Cyber Security

FOR EXHIBITION



PO Box 35, Orange
NSW 2800 Australia

135 Byng Street, Orange
NSW 2800 Australia

P: +61 2 6393 8000
F: +61 2 6393 8199

council@orange.nsw.gov.au
www.orange.nsw.gov.au



All policies can be reviewed or revoked by a resolution of Council, at any time.

TABLE OF CONTENTS

PURPOSE	3
INTRODUCTION	3
ROLES & RESPONSIBILITIES	3
Chief Executive Officer	3
Manager, Information Technology	3
IT Operations Team Leader	4
Council Staff Councillors and General Contractors	4
Manager, Corporate Governance	4
Internal Audit and Risk	4
FOUNDATIONAL REQUIREMENTS	5

FOR EXHIBITION



All policies can be reviewed or revoked by a resolution of Council, at any time.

PURPOSE

This policy outlines the high-level cyber security standards recommended for all NSW Local Government by Cyber Security NSW. It is designed to be read by General Managers/CEOs, Chief Information Officers (or equivalent), Chief Information Security Officers (or equivalent) and Audit and Risk teams.

INTRODUCTION

Strong cyber security is an important component of the NSW Beyond Digital Strategy, enabling the effective use of emerging technologies and ensuring confidence in the services provided by NSW Local Government. Cyber security covers all measures used to protect systems – and information processed, stored or communicated on these systems – from compromise of confidentiality, integrity and availability.

Councils must establish effective cyber security operational policies and procedures and embed cyber security into risk management practices and assurance processes. When cyber security risk management is done well, it reinforces organisational resilience, making entities aware of their risks and helps them make informed decisions in managing those risks. This should be complemented with meaningful training, communications and support across all levels of the council.

RELATED COUNCIL POLICIES/DOCUMENTS

- Operational Procedure OP141 - Overarching Information Security Framework
- Operational Procedure OP142 – Data Privacy and Protection
- Operational Procedure OP143 – Access Control
- Operational Procedure OP144 – IT Security
- Operational Procedure OP145 – IT Acceptable Use
- Operational Procedure OP146 – Cloud Security
- Operational Procedure – IT Disaster Recovery Plan
- Business Continuity Plan

RELATED STATE AND FEDERAL GOVERNMENT POLICIES/DOCUMENTS

- NSW Beyond Digital Strategy
- Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)
- Health Records and Information Privacy Act 2002 (HRIP Act)
- NSW Government Information Classification, Labelling and Handling Guidelines 2020
- NSW Cyber Security Policy (the Policy)
- Australia's Cyber Security Strategy
- The Protective Security Policy Framework
- Information Security Manual

ROLES & RESPONSIBILITIES

Council will have the following roles and responsibilities allocated as part of their cyber security function.

Chief Executive Officer

The CEO is responsible for:

- Appointing or assigning an appropriate senior staff member in the council with the authority to perform the duties outlined in this policy.
- Supporting the council's cyber security plan.
- Ensuring their council develops, implements, and maintains an effective cyber security plan and/or information security plan.
- Determining their council's risk appetite.
- Appropriately resourcing and supporting council cyber security initiatives including training and awareness and continual improvement initiatives to support this policy.

Manager, Information Technology

The Manager Information Technology is responsible for:

- Defining and implementing a cyber security plan that includes consideration of threats, risks and vulnerabilities that impact the protection of the council's information and systems within the council's cyber security risk tolerance.



All policies can be reviewed or revoked by a resolution of Council, at any time.

- Developing a cyber security strategy, architecture, and risk management process and incorporate these into the council's current risk framework and processes.
- Assessing and providing recommendations on any exemptions to council information security policies and standards.
- Attending risk committee meetings.
- Implementing policies, procedures, practices, and tools to assist with the implementation of this policy.
- Collaborating with privacy, audit, information management and risk officers to protect council information and systems.
- Ensuring that all staff understand the cyber security requirements of their roles.
- Ensuring a secure-by-design approach for new initiatives and upgrades to existing systems, including legacy systems.
- Ensuring all staff and providers understand their roles in building and maintaining secure systems.
- Establishing training and awareness programs to increase employees' cyber security capability.
- Managing the budget and funding for the cyber security program.
- Managing the life cycle of cyber security platforms including design, deployment, ongoing operation, and decommissioning.
- Ensuring appropriate management of the availability, capacity and performance of cyber security hardware and applications.
- Providing input and support to regulatory compliance and assurance activities and managing any resultant remedial activity.
- Developing a metrics and assurance framework to measure the effectiveness of controls.
- Providing day-to-day management and oversight of operational delivery.

Council Staff Councillors and General Contractors

Staff, Councillors and all general contractors are responsible for:

- Using and preserve Councils systems and digital assets in a secure way by adhering to security policies and operational standards.
- Familiarising themselves with Councils policies and standards and being aware of their responsibilities under these.
- Complying with the requirements of these policies and related operational standards.
- Report violations or suspected violations of these policies in a timely manner.

Manager, Corporate Governance

The Manager, Corporate Governance is responsible for:

- Acting as a focal point within their agency for all matters related to information management that are required to support cyber security.
- Ensuring that a cyber incident that involved damage or loss is escalated and reported to the appropriate team in Council.

IT Operations Team Leader

The IT Operations Team Leader is responsible for:

- Managing and coordinating the response to cyber security incidents, changing threats, and vulnerabilities.
- Investigating, responding to, and reporting on cyber security events.
- Reporting cyber incidents to the Chief Executive Officer (CEO) and Cyber Security NSW, if appropriate.
- Developing and maintaining cyber security procedures and policies.
- Providing guidance on cyber security risks introduced from business and operational change.



All policies can be reviewed or revoked by a resolution of Council, at any time.







Internal Audit and Risk

The Audit and Risk Committee, and internal staff with a responsibility for audit and risk are responsible for:

- Validating that the cyber security plan meets Council's business goals and objectives and ensuring the plan supports the agency's cyber security strategy.
- Providing assurance regarding the effectiveness of cyber security controls.
- Assisting to ensure the risk framework is applied in assessing cyber security risks and with setting of risk appetite.
- Assisting the Manager, Information Technology in analysing cyber security risks.

FOUNDATIONAL REQUIREMENTS

Outlined below are the foundational requirements for a cyber security operational policy framework (See Related Council Policies/Documents at the end of this policy) that focus on enhancing planning and governance, developing a cyber security culture, safeguarding information and systems, strengthening resilience against attacks and improved reporting.

	 LEAD	 PREPARE	 PREVENT	 DETECT	 RESPOND	 RECOVER
1	Council will implement cyber security planning and governance. Council will:					
1.1	Allocate roles and responsibilities as detailed in this policy.					
1.2	Ensure the CEO is accountable for cyber security including risks, plans and meeting the requirements of this policy. Councils need to consider governance of ICT systems to ensure there are no gaps in cyber security related to items such as video surveillance, alarms, life safety and building management systems that use automated or remotely controlled or monitored assets including industrial Internet of Things (IoT) devices.					
1.3	Develop, implement, and maintain an approved cyber security plan that is integrated with Council's business continuity arrangements. This should include consideration of cyber security threats, risks and vulnerabilities that impact the protection of the council's information, ICT assets and services.					
1.4	Include cyber security in their risk management framework and consider cyber security threats when performing risk assessments.					
1.5	Be accountable for the cyber risks of their ICT service providers and ensure the providers comply with the applicable parts of this policy (Section 2.1) and any other relevant council security policies. This should include providers notifying the council quickly of any suspected or actual security incidents and following reasonable direction from the council arising from incident investigations.					



All policies can be reviewed or revoked by a resolution of Council, at any time.

	LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
2	Council should build and support a cyber security culture across their organisation. Council should:					
2.1	Implement regular cyber security awareness training for all employees and contractors. Ensure that outsourced ICT service providers understand and implement the cyber security requirements of the contract.					
2.2	Increase awareness of cyber security risk across all staff including reporting cyber security risks.					
2.3	Foster a culture where cyber security risk management is an important and valued aspect of decision-making and where cyber security risk management processes are understood and applied.					
2.4	Ensure that people who have access to sensitive or classified information or systems and those with privileged system access have appropriate security screening, and that access is removed when they no longer need to have access, or their employment is terminated.					
2.5	Share information on security threats and intelligence with Cyber Security NSW and cooperate across NSW Local Government and NSW Government to enable management of state-wide cyber risk.					
	LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
3	Council should manage cyber security risks to safeguard and secure our information and systems. Councils must:					
3.1	Implement an Information Security Management System (ISMS), Cyber Security Management System (CSMS) or Cyber Security Framework (CSF), with scope at least covering systems identified as the council's "crown jewels". The ISMS, CSMS or CSF should be compliant with, or modelled on, one or more recognised ICT, OT or IoT standard.					
3.2	Implement the ACSC Essential 8 ¹ .					
3.3	Classify information ² and systems according to their business value (i.e. the impact of loss of confidentiality, integrity or availability), adhere to the requirements of the <i>NSW Government Information Classification Labelling and Handling Guidelines</i> and: <ul style="list-style-type: none"> ○ assign overall responsibility for information asset protection and ownership ○ implement controls according to their classification and relevant laws and regulations ○ identify the council's "crown jewels". 					
3.4	Ensure cyber security requirements are built into procurements and into the early stages of projects and the system development life cycle (SDLC), including agile projects. Any upgrades to existing systems should comply with your organisation's cyber risk tolerance.					
3.5	Ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data including processes for internal fraud detection.					

¹ Strategies set out by the Australian Cyber Security Centre aimed at mitigating Cyber Security Incidents.

² <https://www.digital.nsw.gov.au/policy/managing-data-information/information-classification-handling-and-labeling-guidelines>



All policies can be reviewed or revoked by a resolution of Council, at any time.

	LEAD	PREPARE	PREVENT	DETECT	RESPOND	RECOVER
4	Council should improve their resilience including their ability to rapidly detect cyber incidents and respond appropriately. Council should:					
4.1	Have a current cyber incident response plan that integrates with your business continuity plan.					
4.2	Test their cyber incident response plan every year and involve their senior staff responsible for the management of media and external communications.					
4.3	Deploy monitoring processes and tools to allow for adequate incident identification and response.					
4.4	Report cyber security incidents to the Manager, Information Technology or IT operations Team Leader and Cyber Security NSW.					
4.5	Participate in or observe state-wide cyber security exercises as required.					

ST13 – Strategic Policy – Cyber Security

Review Due: November 2024	Version 1_22	Last Revision: New Policy
Approval by:	Minute Number:	Approval Date: