



BUSINESS PAPER

**Economic and Community
Sustainability Committee Meeting
Wednesday, 11 October 2023**

INVERELL SHIRE COUNCIL**NOTICE OF ECONOMIC AND COMMUNITY SUSTAINABILITY COMMITTEE MEETING**

6 October, 2023

An Economic and Community Sustainability Committee Meeting will be held at the Tingha Town Hall on Wednesday, 11 October, 2023, commencing at **10.30am**.

Your attendance at this Economic and Community Sustainability Committee Meeting would be appreciated.

Please Note: Under the provisions of the Code of Meeting Practice the proceedings of this meeting (including presentations, deputations and debate) will be recorded. The audio recording of the meeting will be uploaded on the Council's website at a later time. Your attendance at this meeting is taken as consent to the possibility that your voice may be recorded and broadcast to the public.

I would like to remind those present that an audio recording of the meeting will be uploaded on the Council's website at a later time and participants should be mindful not to make any defamatory or offensive statements.

P J HENRY PSM

GENERAL MANAGER

Agenda

1	Apologies	5
2	Confirmation of Minutes.....	5
3	Disclosure Of Conflict Of Interests/Pecuniary And Non-Pecuniary Interests	10
4	Destination Reports.....	11
4.1	Request for Donation - Waiver of Copeton Northern Foreshores Community Hall Hire Fee - Charity Event - Tiffany and Janice Pollock.....	11
4.2	Request for Donation - Waiver of Town Hall Hire fees - BreastScreen NSW (Hunter New England Health).....	12
4.3	Privacy and Personal Information Protection Act 1998 Amendments	13
4.4	Referral of Confidential Matters	72
5	Governance Reports.....	73
5.1	Risk Management Framework.....	73
5.2	Governance - Monthly Investment Report	104
6	Confidential Matters (Committee-of-the-Whole)	108
6.1	Outstanding Debtor Account - 215057-1	108

Ethical Decision Making and Conflicts of Interest

A guiding checklist for Councillors, officers and community committees

Ethical decision making

- Is the decision or conduct legal?
- Is it consistent with Government policy, Council's objectives and Code of Conduct?
- What will the outcome be for you, your colleagues, the Council, anyone else?
- Does it raise a conflict of interest?
- Do you stand to gain personally at public expense?
- Can the decision be justified in terms of public interest?
- Would it withstand public scrutiny?

Conflict of interest

A conflict of interest is a clash between private interest and public duty. There are two types of conflict:

- **Pecuniary** – regulated by the *Local Government Act 1993* and Office of Local Government
- **Non-pecuniary** – regulated by Codes of Conduct and policy. ICAC, Ombudsman, Office of Local Government (advice only). If declaring a Non-Pecuniary Conflict of Interest, Councillors can choose to either disclose and vote, disclose and not vote or leave the Chamber.

The test for conflict of interest

- Is it likely I could be influenced by personal interest in carrying out my public duty?
- Would a fair and reasonable person believe I could be so influenced?
- Conflict of interest is closely tied to the layperson's definition of 'corruption' – using public office for private gain.
- Important to consider public perceptions of whether you have a conflict of interest.

Identifying problems

- 1st** Do I have private interests affected by a matter I am officially involved in?
2nd Is my official role one of influence or perceived influence over the matter?
3rd Do my private interests conflict with my official role?

Local Government Act 1993 and Model Code of Conduct

For more detailed definitions refer to Sections 442, 448 and 459 or the *Local Government Act 1993* and Model Code of Conduct, Part 4 – conflicts of interest.

Disclosure of pecuniary interests / non-pecuniary interests

Under the provisions of Section 451(1) of the *Local Government Act 1993* (pecuniary interests) and Part 4 of the Model Code of Conduct prescribed by the Local Government (Discipline) Regulation (conflict of interests) it is necessary for you to disclose the nature of the interest when making a disclosure of a pecuniary interest or a non-pecuniary conflict of interest at a meeting.

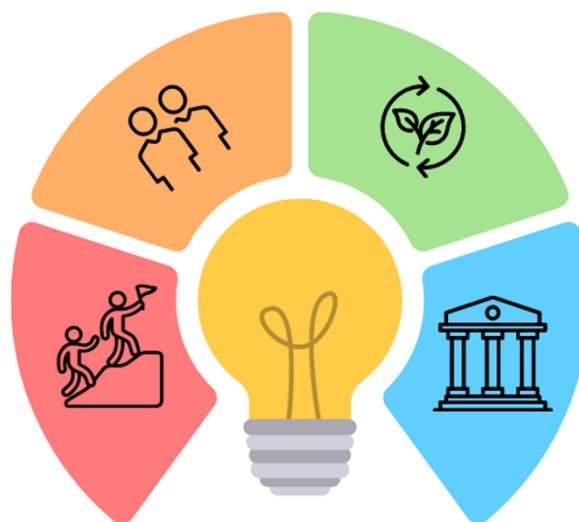
A Declaration form should be completed and handed to the General Manager as soon as practicable once the interest is identified. Declarations are made at Item 3 of the Agenda: Declarations - Pecuniary, Non-Pecuniary and Political Donation Disclosures, and prior to each Item being discussed: The Declaration Forms can be downloaded at [Disclosure of pecuniary interests form](#) or [non-pecuniary interests form](#)

Quick Reference Guide

Below is a legend that is common between the:

- Inverell Shire Council Strategic Plan;
- Inverell Shire Council Delivery Plan; and
- Inverell Shire Council Operational Plan.

OUR DESTINATIONS



01 LEADERSHIP



We will be an accountable and responsible Council that will be involved with the community and responsibly manage public resources.

02 PROSPERITY



The Shire has a diverse, strong local economy that provides opportunities that contribute to the quality of life for the community.

03 LIVEABILITY



Our community is healthy, safe, educated and offers opportunities for people of all ages and abilities. We value our natural and built environment.

04 SERVICES & INFRASTRUCTURE



Our community is enhanced by the provision of civic services and infrastructure. These services are planned and financially sustainable.

1 APOLOGIES

2 CONFIRMATION OF MINUTES

RECOMMENDATION:

That the Minutes of the Economic and Community Sustainability Committee Meeting held on 13 September, 2023, as circulated to members, be confirmed as a true and correct record of that meeting.

**MINUTES OF INVERELL SHIRE COUNCIL
ECONOMIC AND COMMUNITY SUSTAINABILITY COMMITTEE MEETING
HELD AT THE COMMITTEE ROOM, ADMINISTRATIVE CENTRE, 144 OTHO STREET,
INVERELL
ON WEDNESDAY, 13 SEPTEMBER 2023 AT 11.10AM**

PRESENT: Cr Paul King OAM (Chair), Cr Paul Harmon (Mayor), Cr Kate Dight, Cr Di Baker, Cr Wendy Wilks and Cr Jo Williams.

IN ATTENDANCE: Paul Henry (General Manager), Brett McInnes (Director Civil & Environmental Services) and Paul Pay (Director Corporate and Economic Services).

1 APOLOGIES

COMMITTEE RESOLUTION

Moved: Cr Paul Harmon

Seconded: Cr Kate Dight

That the apology received from Cr Nicky Lavender for personal reasons be accepted and leave of absence granted.

CARRIED

2 CONFIRMATION OF MINUTES

COMMITTEE RESOLUTION

Moved: Cr Kate Dight

Seconded: Cr Jo Williams

That the Minutes of the Economic and Community Sustainability Committee Meeting held on 9 August, 2023, as circulated to members, be confirmed as a true and correct record of that meeting.

CARRIED

3 DISCLOSURE OF CONFLICT OF INTERESTS/PECUNIARY AND NON-PECUNIARY INTERESTS

Cr Kate Dight declared a Non-Pecuniary (insignificant) Interest in relation to Item #4.1 Notice of Motion - Murray Darling Association Membership S11.15.17 as Cr Dight is a primary producer with water holdings within the Murray Darling Basin.

4 NOTICES OF BUSINESS

4.1 NOTICE OF MOTION - MURRAY DARLING ASSOCIATION MEMBERSHIP S11.15.17

COMMITTEE RESOLUTION

Moved: Cr Kate Dight

Seconded: Cr Jo Williams

That the Committee Recommends to Council that:

- i. *Inverell Shire Council apply to be a member of the Murray Darling Association; and*
- ii. *Membership be funded from Council's expiring Joint Organisation membership funds.*

CARRIED

5 DESTINATION REPORTS

5.1 REQUEST TO LICENCE - AUTOMATIC WEATHER STATION SITE - RAGLAN STREET, INVERELL - BUREAU OF METEOROLOGY S5.10.65

COMMITTEE RESOLUTION

Moved: Cr Paul Harmon

Seconded: Cr Di Baker

The Committee recommends to Council that:

- i) *Council enter into a Licence Agreement with Commonwealth of Australia as represented by the Bureau of Meteorology for a section of land located in Lot 4 in Deposited Plan 1152029, Raglan Street, Inverell;*
- ii) *the Licence Agreement be for a period of 10 years;*
- iii) *the Licence Fee be \$1.00 excluding GST per annum; and*
- iv) *the Licence Agreement be subject to any other terms and conditions as negotiated by Council's General Manager.*

CARRIED

5.2 REQUEST TO LEASE - MANDOE RADIO SITE - LOT 22 DP 721168 MOUNT HALLAM ROAD, ATHOLWOOD - AMPLITEL PTY LIMITED S5.10.65

COMMITTEE RESOLUTION

Moved: Cr Paul Harmon

Seconded: Cr Kate Dight

That:

1. *Subject to 100 Square Metres of suitable land being available on site, noting that a design visit has not yet been conducted;*
2. *A guarantee from the Amplitel Pty Limited that existing infrastructure on the site will be not be impacted;*

The Committee recommends to Council that:

3. *Council enter into a Lease Agreement with Amplitel Pty Limited for Mandoe Radio Site, Lot 22 DP 721168, Mount Hallam Road, Atholwood for a five (5) year period with an option of 3 further terms of five (5) years;*
4. *the Lease fee be \$7,500 per annum (GST exclusive) with a 3% increase per annum; and*
5. *the Lease Agreement be subject to any other terms and conditions as negotiated by Council's General Manager.*

CARRIED

5.3 MANAGEMENT OF THE LINKING TOGETHER CENTRE S5.11.67**COMMITTEE RESOLUTION**

Moved: Cr Kate Dight

Seconded: Cr Jo Williams

The Committee recommends to Council that:

- a) *the Expression of Interest, submitted by Armajun Aboriginal Health Service, to manage and operate the 'Linking Together Centre' be accepted;*
- b) *the management of the centre be guided by a Memorandum of Understanding (MOU) in the terms outlined in this report; and*
- c) *the MOU be for a (3) year period.*

CARRIED**6 INFORMATION REPORTS****6.1 UPDATE - 2023 RALE RASIC JOEYS MINI WORLD CUP S26.3.21****COMMITTEE RESOLUTION**

Moved: Cr Kate Dight

Seconded: Cr Paul Harmon

That the information report be received and noted.

CARRIED**6.2 RURAL RECOVERY SUPPORT SERVICE S14.18.6/16****COMMITTEE RESOLUTION**

Moved: Cr Kate Dight

Seconded: Cr Jo Williams

That the information report be received and noted.

CARRIED**7 GOVERNANCE REPORTS****7.1 GOVERNANCE - MONTHLY INVESTMENT REPORT S12.12.2****COMMITTEE RESOLUTION**

Moved: Cr Kate Dight

Seconded: Cr Di Baker

The Committee recommends to Council that:

- i) *the report indicating Council's Fund Management position be received and noted; and*
- ii) *the Certification of the Responsible Accounting Officer be noted.*

CARRIED

The Meeting closed at 11.32 am.

3 DISCLOSURE OF CONFLICT OF INTERESTS/PECUNIARY AND NON-PECUNIARY INTERESTS

4 DESTINATION REPORTS

4.1 REQUEST FOR DONATION - WAIVER OF COPETON NORTHERN FORESHORES COMMUNITY HALL HIRE FEE - CHARITY EVENT - TIFFANY AND JANICE POLLOCK

File Number: S12.22.1/16 / 23/32526

Author: Kristy Paton, Corporate Support Officer - Publishing

SUMMARY:

Council is in receipt of a letter from Janice Pollock, Me and Mums Kitchen requesting the hire fee of the Hall at Copeton Northern Foreshores be waived for an event being held to raise money for the Inverell Breast Cancer Support Group.

The committee is requested to consider the request.

RECOMMENDATION:

A matter for the Committee.

COMMENTARY:

A "Dolly Parton Tribute Show" will be held at the Copeton Northern Foreshores Hall on Saturday, 9th March, 2024. The show will feature Donella Waters, a professional Entertainer and a local Artist as a support act. Proceeds from the event will be donated to the Inverell Breast Cancer Support Group.

Tickets will cost \$45 per person and this will include a smorgasbord grazing table, BBQ and the entertainment. Refreshments will be BYO.

To maximise the donation made to the Support Group, Ms Pollock has requested the hire fee for the hall be waived. The cost to hire the hall for the event is \$250.

The Committee is requested to make a determination regarding the request for the hire fee of the Copeton Northern Foreshores Hall to be waived.

RISK ASSESSMENT:

Nil

POLICY IMPLICATIONS:

Nil

CHIEF FINANCIAL OFFICERS COMMENT:

Council's donation budget has funding available of \$49,176 should Council elect to support this event.

LEGAL IMPLICATIONS:

Nil

ATTACHMENTS:

Nil

4.2 REQUEST FOR DONATION - WAIVER OF TOWN HALL HIRE FEES - BREASTSCREEN NSW (HUNTER NEW ENGLAND HEALTH)**File Number:** S12.22.1/16 / 23/32483**Author:** Kristy Paton, Corporate Support Officer - Publishing**SUMMARY:**

Council is in receipt of a Request for Donation Application Form from Belinda Hook, BreastScreen NSW (Hunter New England Health). Ms Hook is requesting the hire fee for the Inverell Town Hall be waived for their event – BreastScreen / “Support the Girls”. The Committee is requested to consider the request.

RECOMMENDATION:

A matter for the Committee.

COMMENTARY:

BreastScreen NSW and the charity “Support the Girls” are combining to run an event in Inverell for Aboriginal women. The event will include a screening along with a bra fitting. The event is to be held on Wednesday, 29 November, 2023 at the Inverell Town Hall and the Turnham carpark.

Mammogram screening for Aboriginal women is lower than it is in the general population and it is hoped this event will raise awareness of the importance of screening for Aboriginal women in the Inverell Community. BreastScreen NSW will be working in conjunction with local health care providers – Healthwise, Armajun and the local Aboriginal Health Unit to plan and deliver screening and health promotion. It is intended the BreastScreen Mobile Unit will be booked for the entire day to maximise the number of screenings (approximately 40 appointments).

The Town Hall will be used as a safe space where women will be provided with a bra fitting, they will also receive a free bra along with toiletries and hygiene products. This will also allow an opportunity for the women to connect with health care workers.

The hire fee for the event is \$560, this includes the use of the main hall and the kitchen/Annex.

The Committee is requested to make a determination regarding the request for the hire fee of the Inverell Town Hall to be waived.

RISK ASSESSMENT:

Nil

POLICY IMPLICATIONS:

Nil

CHIEF FINANCIAL OFFICERS COMMENT:

Council's donation budget has funding available of \$49,176 should Council elect to support this event.

LEGAL IMPLICATIONS:

Nil

ATTACHMENTS:

Nil

4.3 PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998 AMENDMENTS

File Number: S16.11.2 / 23/32935

Author: David Thirlway, Manager Information Services

SUMMARY:

Amendments to the *Privacy and Personal Information Protection Act 1998* will be effective on 28 November 2023.

To meet the mandatory requirements of the amendments, Council needs to review the Privacy Management Plan, adopt a Data Breach Response Policy, and create an Internal Register of eligible data breaches and a Public Notification Register.

RECOMMENDATION:

The Committee recommends to Council that Council adopts the following policies and documents:

- i) Council's Privacy Management Plan;*
- ii) Data Breach Response Policy;*
- iii) Eligible Data Breach Incident Register; and*
- iv) Public Data Breach Notification Register.*

COMMENTARY:

On 28 November, 2022 the New South Wales Government passed amendments to the *Privacy and Personal Information Protection Act 1998* (PIIP Act). The amendments are to come into effect from 28 November, 2023.

Overview of amendments

- Extend the Act to State-owned corporations that are not subject to the *Privacy Act 1988* of the Commonwealth.
- Introduce a scheme for the assessment of data breaches and the mandatory notification of certain data breaches (MNDB) that occur in relation to the access, disclosure or loss of personal information held by public sector agencies.
- Provide for exemptions from mandatory notification in particular circumstances.
- Give the Privacy Commissioner the power to investigate, monitor, audit and report on public sector agencies in relation to the Scheme for the mandatory notification of data breaches, including the power to observe the systems, policies and procedures of a public sector agency.
- Give the Privacy Commissioner the power to give directions to and make guidelines, recommendations and reports about public sector agencies concerning data breaches.
- Require public sector agencies to publish a data breach policy and data breach register.

Who do the reforms apply to?

- Statutory authorities.
- Universities.
- Local Councils.

How do the amendments affect Councils?

Previously, Councils were not mandated to notify data breaches except for breaches to tax file numbers to the Australian Information Commissioner. With the introduction of the changes, Councils are now mandated to notify both the NSW Privacy Commissioner and affected individuals if a data breach is likely to cause serious harm to that individual. Council will now be mandated to comply with MNDB scheme obligations, including procedures and practices to ensure compliance with Part 6A of the Act (MNDB).

The introduction of the amendments also brings new transparency requirements to Councils. These requirements are designed to increase transparency and deter agencies from breaching privacy rights in NSW. Councils will be required to:

- Publish their Data Breach Policy and Privacy Management Plan.
- Establish an internal register of eligible data breaches.
- Implement best privacy practices.
- Establish and publish a public notification register of eligible data breaches.

Council's obligations under the MNDB Scheme

- Immediately make all reasonable efforts to contain a data breach.
- Undertake an assessment within 30 days where there are reasonable grounds to suspect there may have been an eligible data breach.
- During the assessment period, make all reasonable attempts to mitigate the harm done by the suspected breach.
- Decide whether a breach is an eligible data breach or there are reasonable grounds to believe the breach is not an eligible data breach.
- Notify the Privacy Commissioner and affected individuals of the eligible data breach.
- Comply with other data management requirements.

How to achieve compliance

To ensure Council's readiness to achieve compliance with the upcoming legislative changes to the PPIP Act, Information Service has completed the following:

- Assess and remediate existing privacy controls and security using the five privacy domains prescribed by the Australian Privacy Principles (APP): consideration, collection, dealing with, integrity and access and correction (see Attachment 1 for a briefing on findings).
- Review the Privacy Management Plan and make changes to ensure compliance (See Attachment 2 for a revised version to reflect findings from Attachment 1).
- Create a new Data Breach and Response Policy (See Attachment 3).
- Create a new Incident Register – Using recommended fields from the Information and Privacy Commission (see Attachment 4).
- Create a new Public Notification Register – Using recommended fields from the Information and Privacy Commission (see Attachment 5).
- Publish the Privacy Management Plan, Data Breach and Response Policy and Public Notification Register to Council's website.
- Provide privacy education to staff.

Consequences of non-compliance

To date Information Services is not aware of any penalties being imposed for non-compliance to the MNDB scheme. However, the NSW Privacy Commissioner will have corresponding enforcement powers to administer the Scheme and ensure adherence to the Privacy Act.

The Privacy Commission NSW have been contacted and advised that there are no monetary consequences yet; however, more information is being released as the mandated date comes into effect, and a monetary consequence may be introduced.

While there may not be monetary penalties for non-compliance with the MNDB scheme, Councils could face penalties for serious, repeated privacy breaches of individuals. Moreover, non-compliance with data privacy regulations can damage Council's reputation, eroding trust and public confidence and attracting negative media coverage and legal consequences.

Conclusion

To ensure Council meet mandatory requirements with the Notifiable Data Breach scheme before 28 November 2023, it is recommended that Council:

- Update Council's Privacy Management Plan (Attachment 2) to include the recommendations from the privacy assessment brief (Attachment 1).
- Implement a Data Breach Response Policy and make available to the public (Attachment 3).
- Implement an Internal Eligible Data Breach Incident Register (Attachment 4).
- Implement a Public Notification Register of eligible data breaches, available to the public (Attachment 5).

RISK ASSESSMENT:

- Reputational Risk.
- Regulatory compliance.

POLICY IMPLICATIONS:

Nil

CHIEF FINANCIAL OFFICERS COMMENT:

Nil

LEGAL IMPLICATIONS:

Nil

ATTACHMENTS:

1. Privacy Assessment Brief [↓](#)
2. Privacy Management Plan [↓](#)
3. Data Breach Response Policy [↓](#)
4. Eligible Data Breach Incident Register [↓](#)
5. Public Data Breach Notification Register [↓](#)

Inverell Shire Council Privacy Assessment

To ensure compliance with the upcoming legislative changes to the Privacy Act (Cth) 1988 and Notifiable Data Breach scheme, a privacy assessment of Council's existing privacy controls has been completed and a path towards readiness to achieve compliance, using the Australian Privacy Principles as a guide.

In the context of the Council's compliance with privacy regulations, compliance with the Australian Privacy Principles (APPs) demonstrates the commitment to privacy protection. It provides a strong foundation for aligning with the Information Privacy Principles (IPPs) mandated by the Privacy Act.

The APPs underlying principles closely mirror the core tenets of the IPPs applicable to the public sector within NSW. By adhering to the APPs, Council proactively implemented privacy best practices, ensuring transparency, accountability, and the responsible handling of personal information.

The 13 principles outlined in the APPs have been used as a guide while reviewing documents, including policies, procedures, and protocols to access Council's provisions for data privacy. These principles are in line with the key requirements outlined in the IPPs.

The analysis of the five privacy sections (shown below) formed the basis for providing recommendations on how Council can address the deficiencies and bridge the gaps in Council's privacy posture.

Section	APP Categories
Consideration of PI Privacy	APP – 1: Open and Transparent management of Personal Information APP – 2: Anonymity and pseudonymity
Collection of PI	APP – 3: Collection of solicited personal information APP – 4: Dealing with unsolicited information APP – 5: Notification of the collection of personal information
Dealing with PI	APP – 6: Use or disclosure of personal information APP – 7: Direct Marketing APP – 8: Cross-border disclosure of personal information APP – 9: Adoption, use or disclosure of government related identifiers
Integrity of PI	APP – 10: Quality of Personal Information APP – 11: Security of Personal Information
Access & Correction of PI	APP – 12: Access to personal information APP – 13: Correction of personal information

The review was conducted using Council's Privacy Management Plan, Information Technology - Digital Intrusion Security Controls, Data Destruction & Retention Process, and Proof of Identity and Personal and Sensitive Document Register.

Findings from the review have shown Council have 4 areas of concern, and 3 non-conformances.

Based on the assessment the following is recommended to improve the overall status of Council's privacy security and help ensure compliance with the Privacy Act.

Areas of Concern

- Prepare measures to avoid over-collection – The Privacy Management Plan should be updated to provide clear guidance on how to prevent the over-collection of personal information by private contractors or consultants engaged by Council (APP-3.5).
- Notification form for third-party data collection - PPIPA requires Council to take reasonable steps to notify individuals of the collection of their personal information, including the source from which the information was collected, unless an exception applies. Council should develop and implement a notification form that should be readily available and easily accessible to individuals. Exceptions to this requirement should be clearly outlined in the Privacy Management Plan (APP-5.2).
- Disposal log for disposed personal information - Council Records Disposal Log should contain who authorised the disposal of records. A Column to note the who authorised the disposal should be added to the log (APP-11.10).
- Procedures for identifying inaccurate personal information – Council does not have a document or process that guides staff in identifying if personal information is inaccurate, out of date, incomplete, irrelevant or misleading. Council could investigate developing and implementing a Data Quality Management Plan and process to ensure correct data with training to reinforce the importance of maintaining accurate and up-to-date personal information.

Non-conformances

- Procedures for collecting unsolicited information - To ensure compliance with Australian privacy policies, Council should update its Privacy Management Plan to provide clear guidance on the procedures and systems (APP-4.1).
- Prepare data breach response plan – Council should have a data breach response Policy/Plan as a best practice to handle personal information. It will help to mitigate the impact of a breach, comply with regulatory requirements, maintain public trust, improve preparedness, and enhance organisational resilience. The Privacy Management Plan should be updated to include information about the data breach and a high-level action list that directs them on how to respond appropriately in similar circumstances (APP-11.7).
- Measures to monitor shared personal information - There is no evidence of a document that captures measures to monitor the protection of the personal information shared with other entities. Privacy policies should include clear guidelines for disclosing personal information to another entity. A data sharing agreement should outline the measures taken to protect personal information during transfer, such as encryption, access controls, and data retention policies. (APP-11.7).

Concluding recommendation

To strengthen Council's privacy security, it is recommended to:

- Prepare and implement a data breach response Policy/Plan.
- Update the Privacy Management Plan to provide clear guidance on dealing with unsolicited personal information, and include clear guidelines for disclosing personal information to another entity.

- Update the Privacy Management Plan to provide clear guidance on measures to avoid over-collection of personal information, including establishing measures to monitor the collection of personal information.



COUNCIL POLICY:	Privacy Management Plan
Ref:	

Contact Officer	Director Corporate Services, Corporate Services
Approval Date	
Approval Authority	Council
Reviewed	Every four years
Amended / Reviewed	
Date of Next Review	



INVERELL SHIRE COUNCIL

PRIVACY MANAGEMENT PLAN FOR LOCAL GOVERNMENT

CONTENTS

Part 1 - Introduction	4
What is personal information?	5
What is health information?	6
Policy on Electoral rolls	6
Application of Plan	6
Personal information held by Council	6
Application for Suppression under 739 LGA	7
Unsolicited information	7
Part 2 – Public Registers	8
Public Registers and PPIPA	8
Effect on section 12 of LGA	9
Where some information in the particular has been published	9
Disclosure of personal information contained in Public Register	9
Purposes of public registers	10
Applications for access to own records on a Public Register	11
Application for suppression in relation to Public register	11
Other registers	11
Part 3 – The Information Protection Principles	12
<u>Privacy and Personal Information Protection Act 1998</u>	
3.1 Information Protection Principle 1	12
3.2 Information Protection Principle 2	13
3.3 Information Protection Principle 3	14
3.4 Information Protection Principle 4	15
3.5 Information Protection Principle 5	16
3.6 Information Protection Principle 6	16
3.7 Information Protection Principle 7	17
3.8 Information Protection Principle 8	18
3.9 Information Protection Principle 9	20
3.10 Information Protection Principle 10	20
3.11 Information Protection Principle 11	22
3.12 Information Protection Principle 12	24
<u>Health Records and Information Privacy Act (HRIPA)</u>	
3.13 Purposes of collection of health information - Principle 1	25
3.14 Information must be relevant - Principle 2	26
3.15 Collection to be from individual concerned - Principle 3	26
3.16 Individual to be made aware of certain matters - Principle 4	27
3.17 Retention and security - Principle 5	28
3.18 Information about health information held by organisations - Principle 6	28
3.19 Access to health information - Principle 7	29
3.20 Amendment to health information - Principle 8	29
3.21 Accuracy - Principle 9	29
3.22 Limits on use of health information - Principle 10	29
3.23 Limits on disclosure of health information - Principle 11	29
3.24 Identifiers - Principle 12	30
3.25 Anonymity - Principle 13	30
3.26 Transborder data flows and data flow to Commonwealth agencies - Principle 14	30
3.27 Linkage to health records - Principle 15	30

Part 4 – Implementation of Privacy Management Plan	31
Training / Induction	31
Responsibilities of Privacy Contact Officer	31
Distribution of information to the public	31
Part 5 - Data Breach	32
Part 6 - Internal Review	33
Part 7 - Other Relevant Matters	34
Appendices	
Appendix 1 – Statutory Declaration for Access under section 57 to a Public Register	35
Appendix 2 – Privacy Notification Form for Post – Collection	36
Appendix 2a – Privacy Notification Form for Post – Collection from other sources	37
Appendix 3 – Privacy Notification Form for Pre – Collection	38
Appendix 4 – Application under section 13	39
Appendix 5 – Application for Access under section 14	40
Appendix 6 – Application for Alteration under section 15	41

1. Introduction

The Privacy and Personal Information Protection Act 1998 ("PPIPA") provides for the protection of personal information and for the protection of the privacy of individuals.

Section 33 of the PPIPA requires all councils to prepare a Privacy Management Plan (the "Plan") to deal with:

- ◆ the devising of policies and practices to ensure compliance by the Council with the requirements of the PPIPA,
- ◆ the dissemination of those policies and practices to persons within the Council,
- ◆ the procedures that the Council proposes for Internal review of privacy complaints;
- ◆ such other matters as are considered relevant by the Council in relation to privacy and the protection of personal information held by it.

This Plan has been prepared for the purpose of section 33 of the PPIPA.

The Act provides for the protection of personal information and health information by means of Information Protection Principles. Those principles are listed below:

Privacy & Personal Information Protection Act (PPIPA)

Principle 1 - Collection of personal information for lawful purposes
Principle 2 - Collection of personal information directly from the individual
Principle 3 - Requirements when collecting personal information
Principle 4 - Other requirements relating to collection of personal information
Principle 5 - Retention and security of personal information
Principle 6 - Information about personal information held by agencies
Principle 7 - Access to personal information held by agencies
Principle 8 - Alteration of personal information
Principle 9 - Agency must check accuracy of personal information before use
Principle 10 - Limits on use of personal information
Principle 11 - Limits on disclosure of personal information
Principle 12 - Special restrictions on disclosure of personal information

Health Records and Information Privacy Act (HRIPA)

Principle 1 - Purposes of collection of health information
Principle 2 - Information must be relevant, not excessive, accurate and not intrusive
Principle 3 - Collection to be from individual concerned
Principle 4 - Individual to be made aware of certain matters
Principle 5 - Retention and security
Principle 6 - Information about health information held by organisations
Principle 7 - Access to health information
Principle 8 - Amendment to health information
Principle 9 - Accuracy
Principle 10 - Limits on use of health information
Principle 11 - Limits on disclosure of health information
Principle 12 - Identifiers
Principle 13 - Anonymity
Principle 14 - Transborder data flows and data flow to Commonwealth agencies
Principle 15 - Linkage to health records

Those principles are *modified* by the Privacy Code of Practice for Local Government ("the Code") made by the Attorney General.

The Code has been developed to enable Local Government to fulfil its statutory duties and functions under the Local Government Act 1993 (the "LGA") in a manner that seeks to comply with the PPIPA and HRIPA.

This Plan outlines how the Council will incorporate the 12 PIPPA and 15 HRIPA Information Protection Principles into its everyday functions.

This Plan should be read in conjunction with the Code of Practice for Local Government.

Nothing in this Plan is to affect:

- ◆ any matter of interpretation of the Code or the Information Protection Principles as they apply to the Council;
- ◆ any obligation at law cast upon the Council by way of representation or holding out in any manner whatsoever;
- ◆ create, extend or lessen any obligation at law which the Council may have.

This Plan is designed to introduce policies and procedures to maximise compliance with the PPIPA and HRIPA.

Where the Council has the benefit of an exemption, it will nevertheless describe procedures for compliance in this Plan. By doing so, it is not to be bound in a manner other than that prescribed by the Code.

Council collects, stores and uses a broad range of information. A significant part of that information is personal information. This Plan applies to that part of the Council's information that is personal information.

It may mean in practice that any information that is not personal information will receive treatment of a higher standard; namely treatment accorded to personal information where the information cannot be meaningfully or practicably separated.

What is personal information?

"Personal information" is defined in section 4 of the PPIPA as follows:

'Personal information is defined to mean information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This information can be on a database and does not necessarily have to be recorded in a material form'.

What is not "personal information".

"Personal information" does not "include information about an individual that is contained in a publicly available publication". Personal information, once it is contained in a publicly available publication, ceases to be covered by the PPIPA.

Where the Council is requested to provide access or make a disclosure and that information has already been published, then the Council will rely on the provisions of the relevant Act that authorises Council to hold that information and not the PPIPA (for example, section 12(1) of the LGA).

Council considers the following to be publicly available publications:

- ◆ An advertisement containing personal information in a local, city or national newspaper.
- ◆ Personal information on the Internet.
- ◆ Books or magazines that are printed and distributed broadly to the general public.
- ◆ Council Business papers or that part that is available to the general public.
- ◆ Personal information that may be a part of a public display on view to the general public.

Information published in this way ceases to be covered by the PPIPA.

However, Council's decision to publish in this way must be in accordance with PPIPA.

What is health information?

"Health information" is defined in Section 6 of HRIPA as:

- (a) *personal information that is information or an opinion about:*
 - (i) *the physical or mental health or disability (at any time) of an individual, or*
 - (ii) *an individual's express wishes about the future provision of health services to him or her, or*
 - (iii) *a health service provided, or to be provided, to an individual, or*
- (b) *other personal information collected to provide, or in providing, a health service, or*
- (c) *other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or*
- (d) *other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual, but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the HRIPA generally or for the purposes of specified provisions of the HRIPA.*

Policy on Electoral Rolls

The Electoral Roll is a publicly available publication. Council will provide open access to the Electoral Roll in Council's library. Council will refer any requests for copies of the Electoral Roll to the State Electoral Commissioner.

Application of this Plan

The PPIPA, HRIPA and this Plan apply, wherever practicable, to:

- ◆ Councillors;
- ◆ Council employees;
- ◆ Consultants and contractors of the Council;
- ◆ Council owned businesses; and
- ◆ Council committees (including those which may be established under section 355 of the LGA).

Council will ensure that all such parties are made aware that they must comply with PPIPA, HRIPA, the Code of Practice for Local Government, any other applicable Privacy Code of Practice and this Plan.

Personal Information Held by Council

The Council holds personal information concerning Councillors, such as:

- personal contact information;
- complaints and disciplinary matters;
- pecuniary interest returns;
- CCTV video surveillance footage; and
- entitlements to fees, expenses and facilities.

The Council holds personal information concerning its customers, ratepayers and residents, such as:

- CCTV video surveillance footage;
- rates records; and
- DA applications and objections.

The Council holds personal information concerning its employees, such as:

- recruitment material;
- leave and payroll data;
- personal contact information;
- performance management plans;
- disciplinary matters;
- pecuniary interest returns;

- CCTV video surveillance footage; and
- wage and salary entitlements.

Applications for suppression in relation to general information (not public registers).

Where an application for suppression is made in relation to anything other than a public register, then an application under section 739 of the Local Government Act 1993 ("LGA") is required.

Section 739 of the LGA covers all publicly available material under section 12(1) and 12(6) of the LGA other than public registers. As such, it limits disclosure in those circumstances where an application for suppression is successful. An application for suppression must be verified by statutory declaration and otherwise meet the requirements of section 739. When in doubt, Council will err in favour of suppression.

For more information regarding disclosure of information (other than public registers) see the discussion of IPPs 11 and 12 in Part 3 of this Plan.

For information regarding suppression of information on *public registers*, see Part 2 of this Plan.

Caution as to Unsolicited Information

Where an individual, a group or committee, not established by Council, gives Council unsolicited personal information, then that information should be still treated in accordance with this Plan, the Code and the PPIPA for the purposes of IPPs 5-12 which relate to storage, access, use and disclosure of information.

In the event that the council receives unsolicited personal information, the following steps should be taken:

- The council where possible will record the details of the information received, including the source and the date it was received.
- The council will assess whether the information is necessary for the council's functions or activities. If it is not, the information will be securely disposed of.
- If the information is necessary for the council's functions or activities, the council will take reasonable steps to ensure that the information is accurate, up-to-date, complete and relevant before using or disclosing it.
- If the council is unable to determine whether the information is necessary, it will be retained for a reasonable period of time to allow for further assessment before deciding whether to keep or dispose of it.
- The council also ensure that all staff are aware of the procedures for dealing with unsolicited personal information and are trained to follow them.

2. Public Registers

A public register is defined in section 3 of the PPIPA:

'public register means a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)'.

A distinction needs to be drawn between "public registers" within the meaning of Part 6 of the PPIPA and "non public registers". A "non public register" is a register but it is not a "public register" for the purposes of the PPIPA. For example, the register might not be publicly available or it may not contain personal information.

Disclosure in relation to public registers must comply with Part 6 of the PPIPA and the Code. Personal information cannot be accessed by a person about another person unless the personal information is contained in a public register. Where personal information is contained in a public register, then Part 6 of the PPIPA applies to determine whether access to that information will be given to another person.

Disclosure in relation to all other personal information must comply with the Information Protection Principles as outlined in Part 2 of this Plan and the Code where it includes personal information that is not published.

The Council holds the following public registers under the LGA: ***

- ◆ Section 53 - Land Register
- ◆ Section 113 - Records of Approvals
- ◆ Section 449 -450A - Register of Pecuniary Interests
- ◆ Section 602 - Rates Record

***Note – this is purely indicative. Council may, by virtue of its own practice, hold other Public Registers, to which PPIPA applies.

Council holds the following public registers under the Environmental Planning and Assessment Act:

- ◆ Section 100 – Register of consents and approvals
- ◆ Section 149G – Record of building certificates

Council holds the following public register under the Protection of the Environment (Operations) Act:

- ◆ Section 308 – Public register of licences held

Council holds the following public register under the Impounding Act 1993:

- ◆ Section 30 & 31 – Record of impounding

Members of the public may enquire only in accordance with the primary purpose of any of these registers. The primary purpose for each of these public registers is set out in the sections that follow.

Public Registers and the PPIPA

A public register generally confers specific rights or privileges, a benefit, or status, which would not otherwise exist. It may be required by law to be made publicly available or open to public inspection, or it is simply made publicly available or open to public inspection (whether or not payment is required).

Section 57 of the PPIPA requires very stringent controls over the disclosure of personal information contained in a public register. Section 57 provides broadly that where Council is responsible for keeping a public register, it will not disclose any personal information kept in that register unless it is satisfied that the information is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.

Section 57 (2) requires Council to comply to ensure that any person who applies to inspect personal information contained in the public register to give particulars in the form of a statutory declaration as to the proposed use of that information. (Form at Appendix 1 may be used as a guide)

If the stated purpose of the applicant does not conform with the purpose for which the public register is kept, access to the information sought will not be given.

Where personal information is contained in a publicly available publication, that information will not be regarded as personal information covered by the PPIPA.

Public Registers and HRIPA

No public registers held by Inverell Shire Council contain health information.

Effect on Section 12 of the LGA

Section 57 of the PPIPA prevails over section 12 of the LGA to the extent of any inconsistency. Therefore:

1. If a register is listed in section 12(1) of the LGA, access must not be given except in accordance with section 57(1) of the PPIPA.
2. If a register is not listed in section 12(1) of the LGA, access must not be given except:
 - (i) if it is allowed under section 57(1) of the PPIPA; **and**
 - (ii) inspection would not be contrary to the public interest as per section 12(6) of the LGA.

Note: Both 1 and 2 are amended with regard to specific public registers in the Privacy Code of Practice for Local Government.

Where some information in the public register has been published

That part of a public register that is not published in a publicly available publication will be treated as a "public register" and the following procedure for disclosure will apply.

For example, the Register of Consents and Approvals held by Council under section 100 of the Environmental Planning and Assessment Act requires Council to advertise or publish applications for development consent.

When Council publishes the address of the property, it may identify the owner. The personal information that has not been published and any applications not advertised or that have been rejected or withdrawn (and hence also not published) will be treated as a public register under PPIPA.

Council may hold a register under the Contaminated Land Management Act on behalf of the Environment Protection Authority. This is not to be considered a public register of the Council as the statute does not place any obligations on the Council to make this register publicly available as a register of contaminated land. Furthermore, the legislation foreshadows that the Environment Protection Authority may indeed post this list or register on the internet. This may constitute a publication of the information and therefore the PPIPA will not apply.

Registers should not be published on the internet.

Disclosure of personal information contained in the public registers

A person seeking a disclosure concerning someone else's personal information from a public register must satisfy Council that the intended use of the information is for a purpose relating to the purpose of the register or the Act under which the register is kept.

In the following section, by way of guidance only, what might be called the "primary" purpose (or "the purpose of the register") has been specified for each identified register. In some cases a "secondary purpose" has also been specified, by way of guidance as to what might constitute "a purpose relating to the purpose of the register".

Purposes of Public Registers**Purposes of public registers under the Local Government Act**

Section 53 - Land Register – The primary purpose is to identify all land vested in Council, or under its control. The secondary purpose includes a consideration of public accountability as to the land held by Council. Third party access is therefore a secondary purpose.

Section 113 - Records of Approvals – The primary purpose is to identify all approvals granted under the LGA.

Section 450A - Register of Pecuniary Interests – The primary purpose of this register is to determine whether or not a Councillor or a member of a council committee has a pecuniary interest in any matter with which the council is likely to be concerned. There is a corresponding public accountability purpose and third party access is a secondary purpose.

Section 602 - Rates Record - The primary purpose is to record the value of a parcel of land and record rate liability in respect of that land. The secondary purpose includes recording the owner or lessee of each parcel of land. For example, that a disclosure on a section 603 (of the LGA) rating certificate that a previous owner was a pensioner is considered to be allowed, because the secondary purpose is "a purpose relating to the purpose of the register".

Purposes of public registers under the Environmental Planning and Assessment Act

Section 100 – Register of consents and approvals – The primary purpose is to identify applications for development consent and other approvals, confirm determinations on appeal and identify applications for complying development certificates.

Section 149G – Record of building certificates – The primary purpose is to identify all building certificates.

Purposes of public registers under the Protection of the Environment (Operations) Act

Section 308 – Public register of licences held – The primary purpose is to identify all licences granted under the Act.

Purposes of the public register under the Impounding Act

Section 30 & 31 – Record of impounding – The primary purpose is to identify any impounding action by Council.

Secondary purpose of all Public Registers

Due to the general emphasis (to be found in the LGA and elsewhere) on local government processes and information being open and accountable, it is considered that a secondary purpose for which all public registers are held by Council includes the provision of access to members of the public. Therefore disclosure of specific records from public registers would normally be considered to be allowable under section 57 of the PPIPA.

However, requests for access, copying or the sale of the whole or a substantial part of a Public Register held by Council will not necessarily fit within this purpose. Council should be guided by the Privacy Code of Practice for Local Government in this respect. Where Council officers have doubt as to the intended use of the information, an applicant may be requested to provide a statutory declaration so that Council may satisfy itself as to the intended use of the information.

Council will make its assessment as to the **minimum** amount of personal information that is required to be disclosed with regard to any request.

Other Purposes

Persons or organisations who apply to Council to have access to the information contained in any public register for a purpose not related to the purpose of the register, may be given access at the discretion of Council but only in accordance with the Privacy Code of Practice for Local Government concerning Public

Registers.

Applications for access to own records on a public register

A person wishing to have access to a public register to confirm their own details needs only to prove their identity to Council before having access to their own personal information.

Applications for suppression in relation to a public register

An application for suppression in relation to a public register will be dealt with under PPIPA, rather than section 739 of the LGA.

A person about whom personal information is contained (or proposed to be contained) in a public register, may request Council under section 58 of the PPIPA to have the information removed from, or not placed on the register.

If Council is satisfied that the safety or well-being of any person would be affected by not suppressing the personal information as requested, Council will suppress the information in accordance with the request unless Council is of the opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing the information, in accordance with section 58(2) of the PPIPA. ("Well-being" is defined in the Macquarie Dictionary as "the good or satisfactory condition of existence; welfare".)

When in doubt, Council will err in favour of suppression.

Any information that is removed from, or not placed on, that aspect of a public register to be made public may be kept on the register for other purposes. That is, the information may still be used for council functions, but it cannot be disclosed to other parties.

An application for suppression should be made in writing addressed to the General Manager and must outline the reasons for the request. The Council may require supporting documentation where appropriate.

Other registers

Council may have other registers that are not public registers. The Information Protection Principles, this Plan, any applicable Code and the Act apply to those registers or databases.

Part 3 – The Information Protection Principles**Privacy and Personal Information Protection Act 1998****3.1 Principle 1 Collection for Lawful Purposes**The Privacy Code of Practice for Local Government

There is no intention to depart from this principle otherwise than is permitted by the PPIPA, or any other Privacy Code of Practice which may apply to Council from time to time.

Inverell Shire Council Policy

Council will only collect personal information for a lawful purpose as part of its proper functions. The LGA governs Council's major obligations and functions.

Section 22 of the LGA provides other functions under other Acts. Some of those Acts are as follows:

Companion Animals Act 1998
Environmental Planning and Assessment Act 1979
Impounding Act 1993
Swimming Pools Act 1992
Environmental Offences and Penalties Act 1989
Freedom of Information Act 1989
Heritage Act 1977
Unhealthy Building Land Act 1990

Council performs a number of functions under a wide range of legislation as provided in Section 22 of the LGA. Additionally, the exercise by Council of its functions under the LGA may also be modified by the provisions of other Acts.

The circumstances under which Council may collect information, including personal information, are varied and numerous. Council will not collect any more personal information than is reasonably necessary for it to fulfil its functions.

Anyone engaged by Council as a private contractor or consultant that involves the collection of personal information, must agree not to collect personal information by any unlawful means. This will include debt recovery actions by or undertaken on behalf of Council by commercial agents.

The private contractor or consultant shall only collect personal information that is necessary for the purposes of the contract signed with the council and will not collect more information than is required. In the event that they are found to be over-collecting personal information, the council reserves the right to terminate the contract in accordance with the termination clause of the signed agreement and/or take legal action under the Privacy Act 1988 (Cth), specifically section 13G, which deals with serious or repeated interference with privacy.

Council will continue to collect and deliver personal information to and from government departments involved in the normal functions of Council's operation. Council will also continue the practice of dealing with the NSW Department of Community Services (DoCS) for enquiries on personnel and recruitment matters ie. pre-employment screening of people working with children (Children and Young Peoples Act).

Council will use personal information for a variety of purposes within its departments. Whilst the information was collected for 1 main purpose, it may be used for a variety of other purposes. Eg. the names and addresses of individual owners of property kept on the Rates & Charges Register are used to notify adjoining owners of proposed development, identify companion animal ownership, evaluate road openings and obstructions, evaluate tree preservation orders, investigate parking controls, evaluate land dedications and laneway status, as well as being the basis of the Rates & Charges Register.

In order to ensure compliance with IPP 1, internet contact forms, rates notices, application forms or written requests by which personal information is collected by Council; will be reviewed by the relevant manager prior to adoption, change or use.

Managers are to consider:

- whether the personal information is collected for a lawful purpose
- if that lawful purpose is directly related to a function of Council
- whether or not the collection of that personal information is reasonably necessary for the specified purpose.

3.2 Principle 2 Collection directly from the Individual

The Privacy Code of Practice for Local Government

The Code makes provision for Council to depart from this principle where indirect collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be conferred upon the person to whom the information relates.

Council may wish to confer a special award, prize, benefit or similar form of personal recognition to an individual. This may take the form of a citizen of the year award, the naming of a park after that individual or other similar form of public recognition.

Investigative Code of Practice

Where Council is conducting an investigation, the Investigative Code of Practice prepared by Privacy NSW and approved by the Attorney General, will apply.

IPP 2 is modified by the Investigative Code of Practice to permit indirect collection where a direct collection is reasonably likely to detrimentally affect Council's conduct of any lawful investigation.

Inverell Shire Council Policy

The compilation or referral of registers and rolls are the major means by which the Council collects personal information. For example, the information the Council receives from the Land Titles Office would fit within Section 9(a) PPIPA.

Personal information is also collected from forms completed by customers for development consent, companion animal registration, applications for specific inspections or certifications or applications in respect of tree preservation orders.

Council will treat the personal information contained in petitions in accordance with Section 9 PPIPA. Where Council or a Councillor requests or requires information from individuals or groups, that information will also be treated in accordance with Section 9 PPIPA.

Council regards all personal information concerning its customers as information protected by PPIPA. Council will therefore, collect all personal information directly from its customers except as provided in Section 9(a) PPIPA or under other statutory exemptions or Codes of Practice. Council may collect personal information from other public sector agencies in respect of specific statutory obligations where it is authorised by law to do so.

Where Council anticipates the need to collect personal information indirectly, and not in accordance with this policy, it will first obtain the authorisation of each individual under Section 9(a) PPIPA.

Statutory Exemptions

Compliance with IPP 2 is subject to certain exemptions under the Act. The statutory exemption will be relied upon only in very obvious and limited circumstances and legal advice should normally be obtained.

The relevant statutory exemptions follow:

Section 23(2) PPIPA permits non-compliance with IPP 2 if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal.

Section 24(4) PPIPA permits non-compliance by Council with IPP 2 if:

- investigating a complaint that could be referred or made to, or has been referred from or made by, an investigative agency
- if compliance might detrimentally affect (or prevent the exercise of) the Council's complaint handling or investigative functions.

Section 25(a) and (b) PPIPA permits non-compliance with IPP 2 where the agency is lawfully authorised or required not to comply with the principle by any other Act or law.

Section 26(1) PPIPA permits non-compliance with IPP 2 if compliance would prejudice the interests of the individual concerned.

Discussion

Where Council cannot collect personal information directly from the person, it will ensure 1 of the following:

- Council has obtained authority from the person under Section 9(a) PPIPA.
- The collection of personal information from a third party is permitted under an Act or law. The collection of personal information about a person from a parent or guardian is permitted provided the information relates to a person who is less than 16 years of age.
- The collection of personal information indirectly where one of the above exemptions applies.
- The collection of personal information indirectly is permitted under the Privacy Code of Practice for Local Government or the Investigative Code of Practice.

The only other exception to the above is in the case where Council is provided unsolicited information. In this instance, that information will be treated in accordance with this Plan, the Code and the principles of HRIPA and PPIPA.

3.3 Principle 3 Requirements when Collecting Information

Privacy Code of Practice Local Government

The Code makes provision for Council to depart from this principle where personal information is collected about an individual for the purpose of conferring upon that person, an award, prize, benefit or similar form of personal recognition without prior or subsequent notification.

Investigative Code of Practice

Where Council is conducting an investigation, the Investigative Code of Practice prepared by Privacy NSW and approved by the Attorney General, will apply.

IPP 3 is modified by the Investigative Code to permit non-compliance if compliance is reasonably likely to detrimentally affect (or prevent the proper exercise of) Council's conduct of any lawful investigation.

Inverell Shire Council Policy

Where Council proposes to collect personal information directly from the person, it will inform that person that the personal information is being collected, what is done with that information and who the intended recipients will be.

Council will inform persons if the information is required by law or voluntarily given. In order to address the requirements of Section 10 PPIPA, Council will provide the Pre-collection Privacy Notification Form as appropriate (**Attachment 3**).

A Privacy Protection Notice will be added to all forms where the Council solicits personal information from the general public. Forms used for internal communication will not be effected.

As a minimum, the following application procedures will require a Privacy Notification Form to be in accordance with Section 10 PPIPA:

- Lodging Development Applications
- Lodging comments to Development Applications
- Lodging applications for approval under the LGA
- Any stamps or printed slips that contain the appropriate wording for notification under Section 10
- When collecting an impounded item

In relation to the Privacy Notification Form that may be attached to a Development Application provided to the public, objectors have a right to remain anonymous if they so choose. However, should they need to substantiate their objections, anonymous objections may give less weight (or no weight) in the overall consideration of the Application.

Statutory Exemptions

Where Council collects personal information indirectly from another public sector agency in respect of anyone of its statutory functions, it will advise those individuals that it has collected their personal information in writing. A common example of the collection of information from another public sector agency is the Land Titles Office. Council receives information as to new ownership changes when property ownership is transferred. **Attachment 3** contains a Privacy Notification Form that will be used for post-collection.

Council's compliance with IPP 3 is subject to certain exemptions under the Act. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

The relevant statutory exemptions follow:

Section 23(3) permits non-compliance with IPP 3 where information is collected for law enforcement purposes. Law enforcement means a breach of the criminal law and criminal law enforcement. This Section does not remove the rights of an accused person.

Section 24(4) PPIPA permit non-compliance with IPP 3 if:

- investigation a complaint that could be referred or made to, or has been referred from or made by an investigative agency; and
- if compliance does not detrimentally affect (or prevent the exercise of) the Council's complaint handling or investigative functions.

Section 25(a) and (b) PPIPA permits non-compliance with IPP 3 where the agency is lawfully authorised or required not to comply with the principle by any other Act or law.

Section 26 (1) PPIPA permits non-compliance with IPP 3 if compliance would prejudice the interests of the individual concerned.

Section 26(2) PPIPA permits non-compliance where the person expressly consents to such non-compliance.

3.4 Principle 4 Other requirements relating to Collection

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Inverell Shire Council Policy

Council will seek to ensure that no personal information is collected which is not directly relevant to its proper functions.

Council collects personal information through the various forms that customers may complete and lodge with Council. Before adoption of a new form, a draft form will be reviewed for compliance with IPP 4 by the EEO Officer, Council's legal advisor(s), Public Officer or other suitable person. Should Council have any residual doubts, the opinion of Privacy NSW will be sought.

Council will use public place video surveillance in accordance with *NSW Government Policy Statement and Guidelines for the Establishment and Implementation of Closed Circuit Television in Public Places*. The provisions of the Workplace Surveillance Act will be complied with.

3.5 Principle 5 Retention and Security

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Inverell Shire Council Policy

Council will comply with this principle by using any or all of the following documents:

Code of Conduct
Use of Internet & Email Policy
Records Management Policy
General Records Disposal Schedule for Local Government (GDA 10)

The culling and destruction of records is carried out by the Records Officer in accordance with the Council's Records Management Disposal Schedule. The Records Disposal Schedule is available for public inspection. The Records Officer routinely culls files on a 6 monthly basis for reasons of space and provisions in the Records Management Plan.

Section 12 Information Access Request Forms will be destroyed when each application is completed and any amendments to personal information, rectified.

3.6 Principle 6 Information held by Agencies

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Investigative Code of Practice

Where Council is disclosing personal information to conduct an investigation, disclosure will be allowed under Section 41 of PPIPA by a Direction made by the Privacy Commissioner on 31 December 2005 until such as a Investigative Code of Practice is approved by the Attorney General.

IPP 6 is modified by the Investigative Code to permit non compliance if compliance is reasonably likely to detrimentally affect (or prevent the proper exercise of) Council's conduct of any lawful investigation.

Inverell Shire Council Policy

Council will take all reasonable steps to enable a person to determine whether the council holds personal information about them. If Council holds any information about a person, upon request it will advise them the nature of that information, the main purposes for which it is held, and that person's entitlement to access.

IPP 6 is modified by Section 20(5) PPIPA. Section 20(5) PPIPA has the effect of importing Sections 30-33 and Schedule 1 of the Freedom of Information Act 1989 and treats them as if they were part of PPIPA. That means that in any application under IPP 6, Council must consider the relevant provisions of the FOI Act.

Any person can make application to Council to determine whether personal information is held by completing the appropriate form and submitting it to Council (**Attachment 4**).

Where a person makes an application for access under the PPIPA and it is involved or complex, it may be referred, with the written consent of the applicant, as an application under the FOI Act as a last resort. The applicant has the right to insist on being dealt with under PPIPA.

Where Council receives an application or request by a person as to whether it holds information about them, Council will undertake a search of its records to answer the enquiry. Council may ask the applicant to describe what dealings the applicant has had with Council in order to assist Council to conduct the search.

Council will ordinarily provide a response to applications of this kind within 28 days of the application being made. The fee structure is commensurate to that of the Council's Freedom of Information fees and charges structure.

Statutory Exemptions

Council's compliance with IPP 6 is subject to certain exemptions under the Act. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 25 (a) and (b) PPIPA permits non-compliance with IPP 6 where Council is lawfully authorised or required not to comply with the principle by any other Act or law.

Nothing in this IPP prevents Council from dealing with a request for information about oneself under Section 12 LGA.

3.7 Principle 7 Access to Information held by Agencies

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Investigative Code of Practice

Where Council is disclosing personal information to conduct an investigation, disclosure will be allowed under Section 41 PPIPA by a Direction made by the Privacy Commissioner on 31 December 2005 until such as an Investigative Code of Practice is approved by the Attorney General.

IPP 7 is modified by the Investigative Code to permit non-compliance if compliance is reasonably likely to detrimentally affect (or prevent the proper exercise of) Council's conduct of any lawful investigation.

Inverell Shire Council Policy

IPP 7 requires Council, at the request of any person, to give access to personal information held about them.

Compliance with IPP 7 does not allow disclosure of information about other people. If access to information that relates to someone else is sought, the application must be made under the FOI Act, unless IPPs 11 and 12 or the Public Register provisions apply.

Where a person makes an application for access under PPIPA and it is involved or complex, it may be referred, with the written consent of the applicant, as an application under the FOI Act. The use of the FOI Act provisions in this instance, will be as a last resort and the applicant has the right to insist on being dealt with under PPIPA.

When considering an application under Section 14 PPIPA, Council will consider Sections 30-33 and Schedule 1 of the FOI Act as if they were part of PPIPA.

Customers wishing to exercise their right of access to their own personal information should apply in writing or direct their inquiries to the Privacy Contact Officer, who will make a determination (**Attachment 5**).

Members of staff wishing to exercise their right of access to their personal information should apply in writing on the attached form to have the application dealt with.

In order to comply with the requirement to provide the requested information "without excessive delay or expense", Council will ordinarily provide a response to applications of this kind within 21 days of the application being made, and Council will use a fee structure commensurate to that of the FOI Act fee structure.

Statutory Exemptions

Compliance with IPP 7 is subject to certain exemptions under the Act. If one of those exemptions apply, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 25(a) PPIPA permits non-compliance with IPP 7 where Council is lawfully authorised or required not to comply with the principle.

Section 25(b) PPIPA non-compliance with IPP 7 where non-compliance is "necessarily implied" or "reasonably contemplated" under any Act or law.

Nothing in this principle prevents Council from dealing with a request for information about oneself under Section 12 LGA.

Access to personal information contained in Council Business papers for a "Closed Meeting" should be provided with care to not disclose any other information. Personal information contained in Council Business papers for an "Open Meeting" is published and therefore **not** considered to be covered by the PPIPA.

3.8 Principle 8 Alteration of Personal Information

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Investigative Code of Practice

Where Council is disclosing personal information to conduct an investigation, disclosure will be allowed under Section 41 of PPIPA by a Direction made by the Privacy Commissioner on 31 December 2005 until such as a Investigative Code of Practice is approved by the Attorney General.

IPP 8 is modified by the Investigative Code to permit non-compliance if compliance is reasonably likely to detrimentally affect (or prevent the proper exercise of) Council's conduct of any lawful investigation.

Inverell Shire Council Policy

IPP 8 allows a person to make an application to Council to amend personal information held about them so as to ensure the information is accurate and having regard to the purpose for which the information is collected, relevant to that purpose, up to date and not misleading.

Council wishes to have its information current, accurate and complete. Proposed amendments or changes to the personal information held by the Council are welcomed. However, Council will not provide access under Section 15 PPIPA to information that would not be allowed under Section 14 PPIPA.

Where there are complaints that are or could be the subject of a staff complaint or grievance, they will be referred to the General Manager in the first instance and treated in accordance with the "Grievance and Complaint Handling Procedures".

Any alterations that are or could be the subject of a customer complaint or grievance will be referred to the General Manager, who will make a determination in relation to the matter.

Council has an obligation to take such steps to amend personal information where necessary. If Council decides that it will not amend the information, it must add the additional information, so it can be read with the existing information and the individual notified. The individual to whom the information relates is entitled to have the recipients notified of the amendments made by Council. Incorrect records will be physically altered, whether computerised or in hard copy form. Managers will approve required changes, where applicable. FOI applications may not be required where mistakes are proven quickly.

Where information is requested to be amended, the individual to whom the information relates, must make a request by way of statutory declaration. That request should be accompanied by appropriate evidence as to the cogency of the making of the amendment, sufficient to satisfy the Council that the proposed amendment is factually correct and appropriate. The Council may require further documentary evidence to support certain amendments. Council will not charge to process an application to amend a record under Section 15 PPIPA.

The Council's application form for alteration under IPP 8 is (**Attachment 6**).

If Council is not prepared to amend the personal information in accordance with a request by the individual, the Council may attach to the information in such a manner as is capable of being read with the information, any statement provided by that individual.

If personal information is amended in accordance with IPP 8, the individual to whom the information relates is entitled, if it is reasonably practicable, to have the recipients of that information notified of the amendments made by Council.

The Council will seek to notify recipients of information as soon as possible, of the making of any amendment, where it is reasonably practicable.

Statutory Exemptions

Compliance with IPP 8 is also subject to certain exemptions under the Act. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 25 (a) and (b) PPIPA permits non-compliance with IPP 8 where Council is lawfully authorised or required not to comply with the principle by any other Act or law.

The State Records Act does not allow for the deletion of records however, as a result of Section 20(4) PPIPA, some deletions may be allowed in accordance with IPP 8.

Nothing in PPIPA affects the operation of the *Freedom of Information Act* 1989, and therefore applications to amend records under that Act remain in force as an alternative mechanism.

3.9 Principle 9 Accuracy of Personal Information before Use

The Privacy Code of Practice for Local Government

The Code makes no provision to depart from this principle.

Inverell Shire Council Policy

The steps taken to comply with IPP 9 will depend on the age of the information, its likelihood of change and the particular function for which the information was collected. The more significant the information, the greater the necessity that checks to ensure its accuracy and currency be undertaken prior to its use.

For example, each employee's record should be updated when there is any change of circumstances or when the employee's contact details change.

3.10 Principle 10 Limits on Use

The Privacy Code of Practice for Local Government

The Code makes provision that Council may use personal information for a purpose other than the purpose for which it was created in the following circumstances:

- where the use is in pursuance of Council's lawful and proper function/s and Council is satisfied that the personal information is reasonably necessary for the exercise of such function/s; or
- where personal information is to be used for the purpose of conferring upon a particular person, an award, prize, benefit or similar form of personal recognition.

Council may use personal information obtained for another purpose in pursuance of its lawful and proper functions. For example, the Rates Record that Council holds under Section 602 LGA may also be used to:

- notify neighbours of a proposed development
- evaluate a road opening /closure

Investigative Code of Practice

Where Council is disclosing personal information to conduct an investigation, disclosure will be allowed under Section 41 of PPIPA by a Direction made by the Privacy Commissioner on 31 December 2005 until such as a Investigative Code of Practice is approved by the Attorney General.

IPP 10 is modified by the Investigative Code to permit non-compliance if compliance is reasonably likely to detrimentally affect (or prevent the proper exercise of) Council's conduct of any lawful investigation.

Inverell Shire Council Policy

Council will seek to ensure the information collected for one purpose will be used for that same purpose. Where Council may need to use personal information collected for one purpose, for another purpose in pursuance of its lawful and proper functions, it will first gain the consent of the individual concerned, unless the information to be used is on the Council's public register or an exemption applies.

Statutory Exemption

Compliance with IPP 10 is subject to certain exemptions under the Act. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 23(4) PPIPA permits Council not to comply with IPP 10 where the use of the information for another purpose is reasonably necessary for law enforcement purposes or for the protection of the public revenue. *Law enforcement purposes* means a breach of the criminal law and criminal law enforcement. This Section does not remove the rights of an accused person. *Protection of the public revenue* means, a fraud with respect to taxes or other revenue earning processes such as avoidance of stamp duty.

Section 24 (4) PPIPA permits non-compliance with IPP 10 if:

- investigating a complaint that could be referred or made to, or has been referred from or made by, an investigative agency; and
- if the use is, reasonably necessary in order to enable the Council to exercise its complaint handling or investigative functions.

Section 25 (a) and (b) PPIPA permits non-compliance with IPP 10 where Council is lawfully authorised or required not to comply with the principle by any other Act or law.

Section 28(3) PPIPA permits non-compliance where a disclosure is to be made to a public sector agency under the administration of the Minister for Local Government or a public sector agency under the administration of the Premier for the purpose of informing the Minister (or Premier) about any matter within the Minister's (or Premier's) administration.

The form of consent should include the following elements:

I, (insert name)

of,(insert address)

hereby consent under section 17(2) of the Privacy and Personal Information Protection Act 1998 to Council using the information collected from me by (insert 1st purpose or name of collecting body or person) for the purpose of.....(insert 2nd purpose).

Signed and Dated.....

3.11 Principle 11 Limits on Disclosure

The Privacy Code of Practice for Local Government

The Code makes provision for Council to depart from this principle in the circumstances described below:

Council may disclose personal information to public sector agencies or public utilities on condition that:

- the agency has approached Council in writing;
- Council is satisfied that the information is to be used by that agency for the proper and lawful function/s of that agency, and
- Council is satisfied that the personal information is reasonably necessary for the exercise of that agency's function/s

Where personal information which has been collected about an individual is to be disclosed for the purpose, of conferring upon that person, an award, prize, benefit or similar form of personal recognition.

Where Council is requested by a potential employer, it may verify that a current or former employee works or has worked for Council, the duration of that work, and the position occupied during that time. This exception shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

Investigative Code of Practice

Where Council is disclosing personal information to conduct an investigation, disclosure will be allowed under Section 41 of PIPA by a Direction made by the Privacy Commissioner on 31 December 2005 until such as a Investigative Code of Practice is approved by the Attorney General.

IPP 11 is modified by the Investigative Code to permit non- compliance if disclosure of information is made to another agency that is conducting, or may conduct, a lawful investigation. The information provided must be reasonably necessary for the purposes of that investigation.

Inverell Shire Council Policy

Council will not disclose the information to another person or other body, unless the disclosure is directly related to the purpose for which the information was collected or where the Council has no reason to believe that the individual concerned would object to the disclosure.

Council may disclose personal information to another person or other body where this disclosure is directly related to the purpose for which the personal information was collected and the individual concerned is reasonably likely to have been aware, (or has been made aware in accordance with Section 10 PPIPA), of the intended recipients of that information. "Directly related" can mean the disclosure to another person or agency to deliver a service which supplements that of Councillor disclosure to a consultant for the purpose of assessing or revealing the delivery of a program to which the original collection relates.

The council may disclose personal information to another person or other body where this disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

Statutory Exemptions

Compliance with IPP 11 is subject to certain exemptions under the Act. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 23(5)(a) PPIPA permits non-compliance with IPP 11 where disclosure is made to a law enforcement agency in connection with proceedings for an offence or for law enforcement purposes. *Law enforcement purposes* means a breach of the criminal law and criminal law enforcement. However, Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.

Section 23(5)(b) PPIPA permits non-compliance with IPP 11 where the disclosure is made to a law enforcement agency for the purpose of ascertaining the whereabouts of a person reported to be missing. However, Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.

Section 23(5)(c) PPIPA permits non-compliance with IPP 11 where disclosure is authorised by subpoena, search warrant or other statutory instrument. However Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.

Section 23(5)(d)(i) PPIPA permits non-compliance with IPP 11 where disclosure is reasonably necessary for the protection of the public revenue. *Protection of the public revenue* could mean a fraud with respect to taxes or other revenue earning processes such as avoidance of stamp duty. However Council need not disclose material that it is entitled to refuse in the absence of a subpoena, warrant or other lawful requirement.

Section 23(5)(c)(ii) PPIPA permits non-compliance with IPP 11 where disclosure is reasonably necessary to investigate an offence where there are reasonable grounds to believe an offence has been committed.

Section 24(4) PPIPA permits non-compliance with IPP 11 if:

- investigating a complaint that could be referred or made to, or has been referred from or made by, an investigative agency, and
- if the disclosure is to an investigative agency

Section 25 (a) and (b) PPIPA permits non-compliance with IPP 11 where Council is lawfully authorised or required not to comply with the principle by any other Act or law.

Section 26(2) PPIPA permits non-compliance where the person expressly consents to such non-compliance.

Section 28(3) PPIPA permits non-compliance where a disclosure is to be made to a public sector agency under the administration of the Minister for Local Government or a public sector agency under the administration of the Premier for the purpose of informing the Minister (or Premier) about any matter within the Minister's (or Premier's) administration.

Section 12 LGA overrides Sections 18 and 19 PPIPA to the extent that it lawfully authorises, requires, necessarily implies or reasonably contemplates that councils need not comply with these Sections.

3.12 Principle 12 Special restrictions on Disclosure

The Privacy Code of Practice for Local Government

The Code makes provision for Council to depart from this principle in the circumstances described below:

For the purposes of Section 19(2) only, where Council is requested by a potential employer outside New South Wales, it may verify that a current or former employee works or has worked for Council, the duration of that work, and the position occupied during that time. This exception shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

Investigative of Practice

Where Council is disclosing personal information to conduct an investigation, disclosure will be allowed under Section 41 of PPIPA by a Direction made by the Privacy Commissioner on 31 December 2005 until such as a Investigative Code of Practice is approved by the Attorney General.

The Investigative Code modifies IPP 12 to permit the disclosure of information to another agency that is conducting, or may conduct, a lawful investigation provided the information is reasonably necessary for the purposes of that investigation.

Inverell Shire Council Policy

Council will not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

Statutory Exemptions

Compliance with IPP 12 is also subject to certain exemptions under the Act. If one of those exemptions apply, Council need not comply. The statutory exemption will be relied upon only in limited circumstances and legal advice should normally be obtained.

Section 23(7) PPIPA permits non-compliance with IPP 12 where the disclosure is necessary to investigate an offence or where there are reasonable grounds to believe an offence has been or may be committed.

Section 25 (a) and (b) PPIPA permits non-compliance with IPP 12 where Council is lawfully authorised or required not to comply with the principle by any other Act or law.

Section 26(2) PPIPA permits non-compliance where the person expressly consents to such non-compliance.

Section 28(2) permits non-compliance with IPP 12 where, in the case of health information, the consent of the person cannot reasonably be obtained and the disclosure is made by an authorised person to another authorised person. "Authorised person" means a medical practitioner, health worker, or other official or employee providing health or community services who is employed or engaged by a public sector agency.

Section 28(3) PPIPA permits non-compliance where a disclosure is to be made to a public sector agency under the administration of the Minister for Local Government or a public sector agency under the administration of the Premier for the purpose of informing the Minister (or Premier) about any matter within the Minister's (or Premier's) administration.

Section 12 LGA overrides Sections 18 and 19 PPIPA to the extent that it lawfully authorises, requires, necessarily implies or reasonably contemplates that councils need not comply with these Sections.

Health Records and Information Protection Act 2002

3.13 Principle 1 Collection for Lawful Purposes

All information collection will be carried out under the obligations imposed on Council by its governing legislation and administrative requirements.

Inverell Shire Council Policy

Council will only collect health information for a lawful purpose as part of its proper functions. The LGA governs Council's major obligations and functions. Council will not collect any more health information than is reasonably necessary for it to fulfil its functions.

In very general terms, collection refers to the process by which a person comes into possession of health information. A agency collects health information if it gathers, acquires or obtains information directly from the person to whom it relates or from someone else.

Under the HPPs, the basic standards for collection are:

- only collect health information for a lawful purpose
- only collect health information if it is directly related to Council's activities and necessary for that purpose
- make sure the health information is relevant, accurate and up-to-date and not excessive
- make sure the collection does not unreasonably intrude into the personal affairs of the individual
- collect directly from the person where reasonable and practicable
- inform people you are collecting the health information and why

Under HPP 4(1), Council must take reasonable steps to make sure that the person is aware of the following points:

- the identity of the organisation collecting the information and how to contact them
- the purposes for which the information is collected
- who the Council usually discloses information of that kind to
- any law that requires the particular information to be collected
- the fact that they are able to request access to the information
- the main consequences, if any, for them if all or part of the information is not provided

The meaning of reasonable steps will vary depending on the circumstances of the collection, and what the reasonable person would expect in those circumstances. Where Council collects health information on a form ie. Client Information and Referral Record or Neighbour Aid Home Visiting Service, Council's obligations under Health Privacy Principle 4(1) could be satisfied by a prominent and easy to read statement on that form.

Council must notify the person of the points at or before the time of collection. If that is not practicable, Council must notify the person as soon as practicable after that time.

3.14 Principle 2 Collection to be Relevant

Where information is collected directly from the individual, a statement will appear on the collection instrument to ensure that Council is compliant with this principle.

Inverell Shire Council Policy

In relation to applications for community services purposes the Council will treat the health information contained in these applications in accordance with HRIPA.

Where Council or a Councillor requests or requires information from individuals or groups, that information will be treated in accordance with HRIPA.

Council regards all information concerning its customers as information protected by HRIPA. Council will therefore, collect all health information directly from its customers except as provided in HPP 10 or under other statutory exemptions or Codes of Practice. Council may collect health information from other public sector agencies in respect of specific statutory obligations where it is authorised by law to do so.

Where Council anticipates that it may otherwise need to collect health information indirectly it will first obtain the authorisation of each individual under Section 11(1) HRIPA.

3.15 Principle 3 Collection to be from Individual

Where information is being collected, a statement will appear on the collection instrument to ensure that Council is compliant with this principle.

Inverell Shire Council Policy

Where Council proposes to collect health information directly from the person, it will inform that person that the personal information is being collected, what is done with that information and who the intended recipients will be.

If it is unreasonable or impracticable, Council may need to collect the health information from someone else. Some examples of when it may be unreasonable or impracticable are if the person lacks the capacity to provide their health information, Council may need to collect health information about them from an authorised representative such as, a carer or guardian.

When Council collects a person's health information, Council is required to tell them certain things. This is the case even when collecting health information about them from someone else. At all times, Council must respect the dignity and personal privacy of the person to whom the information relates.

The collection of the person's information as part of the third party's family, social or medical history, is reasonably necessary for the organisation to provide a health service directly to the third party and the person's health information is relevant to the family, medical or social history of the third party.

3.16 Principle 4 Individual to be made aware of Certain Matters

In the process of collecting information, Council will ensure that the information collected is relevant to that purpose, is not excessive and is accurate, up-to-date and complete. Council will ensure the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

Inverell Shire Council Policy

Council will under HPP 4(1) take reasonable steps to make sure that the person is aware of the following points:

- the identity of the organisation collecting the information and how to contact them
- the purposes for which the information is collected
- who the Council usually discloses information of that kind to
- any law that requires the particular information to be collected
- the fact that they are able to request access to the information
- the main consequences, if any, for them if all or part of the information is not provided

The meaning of reasonable steps will vary depending on the circumstances of the collection and what the reasonable person would expect in those circumstances. Council will fulfil its obligations by use of a prominent and easy to read statement on the application form.

In certain circumstances, notifying the person is not necessary or appropriate. Under HPP 4(2) and 4(4) you are not required to notify the person if:

- the person has expressly consented to not being notified
- Council is lawfully authorised or required not to notify the person
- not notifying the person is permitted or is necessarily implied or reasonably contemplated under an Act or any other law
- notifying the person would prejudice their interests
- the information has been collected for law enforcement purposes
- Council is an investigative agency and notifying the person might detrimentally affect or prevent the proper exercise of Council's complaint handling or investigative functions
- Council collects health information about the person from someone else and notifying the person would pose a serious threat to the life or health of any individual

If Council collects health information about the person from someone else, Council may also be able to rely on the notification exemption in Principle 4(3) to not notify the person as long as Council complies with the statutory guidelines.

3.17 Principle 5 Retention and Security

Council will ensure that information is:

- kept no longer than is necessary for the purpose for which the information may lawfully be used through the use of an approved sentencing schedule, disposal authority and storage standard
- disposed of securely and in accordance with any requirements for the retention and disposal of information
- protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse through the use of secure information systems and operational policies and procedures
- only provided to a person in connection with the provision of a service to Council and that everything reasonably within the power of Council is done to prevent unauthorised use or disclosure of the information.

Inverell Shire Council Policy

If Council reasonably believes that the person is incapable of understanding the general nature of the points outlined in HPP 4(1), Council can and should notify any authorised representative of the person instead.

Definition of 'authorised representative'

- (1) In this Act, 'authorised representative' in relation to an individual, means:
 - (a) an attorney for the individual under an enduring power of attorney or
 - (b) a guardian within the meaning of the Guardianship Act 1987 or a person responsible within the meaning of Part 5 of that Act, or
 - (c) a person having parental responsibility for the individual, if the individual is a child or
 - (d) a person who is otherwise empowered under law to exercise any functions as an agent of or in the best interests of the individual.
- (2) A person is not an authorised representative of an individual for the purposes of this Act to the extent that acting as an authorised representative of the individual is inconsistent with an order by a court or tribunal.
- (3) In this section:
'child' means an individual under 18 years of age.
'parental responsibility' in relation to a child, means all the duties, powers, responsibility and authority which, by law, parents have in relation to their children.

Where Council needs to deal with an authorised representative it should still, where practicable, explain the points to the person to whom the information relates in a way that is appropriate to their level of understanding. This is to enable the person to be involved in the notification process to the greatest extent possible.

3.18 Principle 6 Information held by Organisations

Inverell Shire Council Policy

Council will take such steps that are, in the circumstances, reasonable to enable any person to ascertain:

- whether Council holds information relating to that person
- if Council holds information relating to that person the nature of that information, the main purposes for which the information is used and that person's entitlement to gain access to that information.

3.19 Principle 7 Access to Health InformationInverell Shire Council Policy

Council, at the request of the individual to whom the information relates and without excessive delay or expense, will provide the individual with access to the information.

3.20 Principle 8 Amendment to Health InformationInverell Shire Council Policy

Council, at the request of the individual to whom the information relates, will make appropriate amendments (whether by corrections, deletions or additions) to ensure that the information is accurate, relevant, up-to-date, complete and not misleading. Where the information has been collected via other agents, the agent will be requested to amend the information.

If it is not considered appropriate for Council to amend information in accordance with a request by the individual concerned, take reasonable steps to attach to the information any statement provided by that individual of the amendment sought so that this information can be viewed alongside the original information.

In the amendment of information, Council permits the individual to whom the information relates, if it is reasonably practicable, to have recipients of that information notified of the amendments made by Council.

Section 20 HRIPA states:

HPP 8 and any provision of a health privacy code of practice applying to a public sector agency that relates to the requirements set out in that HPP, applies to public sector agencies despite HPP 8(4) and Section 21 of the State Records Act 1998.

3.21 Principle 9 AccuracyInverell Shire Council Policy

Council will not use information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up-to-date, complete and not misleading.

3.22 Principle 10 Limits on UseInverell Shire Council Policy

Where Council collects health information about a person from someone else without notifying the person in accordance with the principles, Council must ensure that any subsequent uses or disclosures it proposes to make of that information are in accordance with these principles. In this regard, Council should recognise that some of the exemptions in the Health Privacy Principles, may be difficult to apply if the person is unaware that their information has been collected.

Example, exemptions based on consent 10(1)(a) and 11(1)(a) and the person reasonably expecting the use or disclosure will generally not be available where the person has not been notified and is not aware that their information has been collected.

3.23 Principle 11 Limits on Disclosure

Council will not disclose information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

- the disclosure is directly related to the purpose for which the information was collected and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure
- the individual concerned is reasonably likely to have been aware or has been made aware that information of that kind is usually disclosed to that other person or body
- Council believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person
- Council believes on reasonable grounds that the disclosure is necessary to assist in an investigation that may lead to prosecution

Inverell Shire Council Policy

Information is disclosed in accordance with the above criteria to a person or body that is a public sector agency or an organisation that is authorised by legislation administered by Council. That agency or organisation shall not use or disclose the information provided by Council for a purpose other than the purpose for which the information was given to it.

3.24 Principle 12 Identifiers

Inverell Shire Council Policy

Council will not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

Individuals are only identified by using unique identifiers if it is reasonably necessary to do so in order to carry out the Council's functions efficiently.

3.25 Principle 13 Anonymity

Inverell Shire Council Policy

Where lawful and practical, individuals are given the opportunity to not identify themselves when entering into transactions with or receiving health services from Council.

3.26 Principle 14 Transferal to Commonwealth Agencies

Inverell Shire Council Policy

Council does not transfer health information outside NSW unless it is in accordance with the conditions set out in HPP 14.

3.27 Principle 15 Linkage to Health Records

Inverell Shire Council Policy

Council endeavours to gain consent before linking health records across more than 1 organisation and only discloses or uses identifiable health information to other organisations with consent.

Part 4 – Implementation of the Privacy Management Plan**Training Seminars/Induction**

During induction, all employees should be made aware that the performance management system has the potential to include personal information on their individual work performance or competency.

Councillors, all staff of the Council including staff of council businesses, and members of council committees should be acquainted with the general provisions of the PPIPA, and in particular, the 12 Information Protection Principles, HRIPA, the Public Register provisions, the Privacy Code of Practice for Local Government, this Plan and any other applicable Code of Practice.

Responsibilities of the Privacy Contact Officer

It is assumed that the Public Officer within Council will be assigned the role of the Privacy Contact Officer unless the General Manager has directed otherwise.

In order to ensure compliance with PPIPA, HRIPA, the Privacy Contact Officer will review all contracts and agreements with consultants and other contractors, rates notices, application forms of whatsoever nature, and other written requests by which personal information is collected by Council, to ensure that Council is in compliance with the PPIPA and HRIPA.

Interim measures to ensure compliance with IPP 3 in particular may include the creation of stamps or printed slips that contain the appropriate wording (see Appendices 2 and 3).

The Privacy Contact Officer will ensure Council in its public areas has special provisions for working with computer screens. Computer screens may require:

- ◆ fast screen savers;
- ◆ face the computers away from the public; or
- ◆ only allow the record system to show one record at a time.

Council's electronic databases should also be reviewed to ensure that they contain procedures and protocols to check the accuracy and currency of personal information.

The Privacy Contact Officer will also provide opinions within Council as to:

- (i) Whether the personal information is collected for a lawful purpose;
- (ii) If that lawful purpose is directly related to a function of Council; and
- (iii) Whether or not the collection of that personal information is reasonably necessary for the specified purpose.

Any further concerns of a legal nature will be referred to Council's solicitor.

Should the Council require, the Privacy Contact Officer may assign designated officers as "Privacy Resource Officers", within the larger departments of Council. In this manner the Council may ensure that the information protection principles are more broadly understood and that individual departments have a greater focus on the information protection principles and are directly applied to Council's day to day functions.

Distribution of information to the public

Council may prepare its own literature such as pamphlets on the PPIPA, HRIPA or it may obtain and distribute copies of literature available from Privacy NSW.

Council may also publish public notices, newsletters or website bulletins explaining the key elements of the Act and the rights of persons about whom information is held. See the discussion in this Plan with respect to IPP 6 for more information in this regard.

The Privacy Contact Officer will ensure that the next available rates notice includes a notice which:

- (i) mentions the commencement of the new PPIPA;
- (ii) states that Council holds personal information;
- (iii) mentions that Council may use and disclose personal information in various circumstances; and
- (iv) states that for further information, please contact the Privacy Contact Officer on (telephone number)

Council may however choose to do a council-wide letterbox drop in preference to (or in addition to) an insert in the rates notices.

Part 5 – Data Breach

5.1 What is Data Breach?

A data breach happens when there is an error that has allowed or could allow unauthorised access to Council's data. Examples include emails sent to the incorrect recipients if they contained classified material or personal information, malware, hacking and data theft, unintentional loss of a paper document, laptop, or USB stick.

5.2 Notifiable Data Breach Scheme (NDB)

5.2.1 Tax File Number collection

As Council collects tax file numbers (TFNs), Council is obligated to fulfil NDB duties in the event of a TFN data breach that is "likely to result in serious harm" to any person. The notification requirements concern notifying both the impacted individuals and the Australian Privacy Commissioner.

5.3 Other Data Breach notification schemes

5.3.1 Sharing of government sector data

The Data Sharing (Government Sector) Act of 2015 (DSGS Act) contains a data breach notification scheme for exchanging government sector data with the other government sector entities under the DSGS Act. If Council receives personal or health information under the DSGS Act and learns that privacy laws have been (or are likely to have been) violated, Council is required to notify the data supplier and the NSW Privacy Commissioner of the violation as soon as practically possible.

5.3.2 European Union's General Data Protection Regulation

The General Data Protection Regulation (GDPR) will apply to any entity that provides products or services to, or monitors the activity of, individuals living in the European Union (EU). The GDPR's requirements for data breach notification include notifying the appropriate EU regulatory authority within 72 hours of becoming aware of the incident.

5.4 Voluntary Notification of Data Breaches

As a matter of best practice, the Information and Privacy Commission (IPC) encourages Council to voluntarily notify their organisation of all additional data breaches, as well as any affected persons, as necessary. This may include data breaches involving TFNs but not other personally identifiable information (PII) or data breaches involving TFNs but

not likely to cause irreparable harm.

The following factors will be taken into consideration by Council when assessing the seriousness of a breach:

- The type of data revealed;
- The disclosure of personal or health information;
- The number of people impacted;
- The risk of harm that the breach could cause to individuals, organisations, and/or Council

Following a determination of the severity of a breach, Council will take the following actions to handle it:

Contain – steps will be taken to contain the breach and minimise any resulting damage.

Evaluate – ascertain the type of data involved in the breach and the risks associated with the breach. This will include an assessment of who is affected by the breach, what was the cause of the breach, and any foreseeable harm to the affected individuals/organisations.

Notify – individuals/organisations affected by the breach will be notified as soon as possible to enable them to take any steps required to protect themselves, and to advise them of their rights to lodge a complaint with the Privacy Commissioner. Council's default position is to voluntarily report data breaches of personal information to the Privacy Commissioner.

Act – any additional action identified to mitigate risks will be implemented.

Prevent – preventive efforts will be put into action based on the type and seriousness of the breach.

Part 6 - Internal Review

How does the process of Internal Review operate?

Complaints are to be made within **6 months** of the complainant being first aware of the conduct. The complaint is to be in writing and addressed to Council's Privacy Contact Officer. The Privacy Contact Officer will appoint a Reviewing Officer to conduct the internal review. The Reviewing Officer must not be substantially involved in any matter relating to the complaint. The Reviewing Officer must be an employee and suitability qualified. The review is to be completed within **60 days** of the lodgement of the complaint. The Council must notify the complainant of the outcome of the review within **14 days** of its determination.

The Privacy Commissioner must be notified of a complaint, briefed on progress and notified of the outcome of an internal review under PPIPA or HRIPA.

What happens after an Internal Review?

If the complainant remains unsatisfied, he/she may appeal to the Administrative Decisions Tribunal which hears the matter afresh and may impose its own decision and award damages for a breach of an information protection principle.

Part 7 – Other Relevant MattersContracts with consultants and other private contractors

It is necessary to have specific provisions to protect the Council in any dealings with private contractors.

Confidentiality

The obligation of confidentiality is additional to and separate from that of privacy. Nevertheless, a duty to withhold information lies at the heart of both concepts. Confidentiality attaches to information per se, personal information to the person to whom that information relates.

An obligation of confidentiality exists for all employees whether express or implied as a matter of law.

Information which may be confidential is also likely to have a separate and independent obligation attaching to it in the form of privacy and in that regard, a release for the purposes of confidentiality will not suffice for privacy purposes. Two separate releases will be required and, in the case of privacy, the person to whom the information relates will be required to provide the release.

Misuse of personal information

Section 664 of the LGA makes it an offence for anyone to disclose information except in accordance with that section. Whether or not a particular disclosure is made with lawful excuse is a matter that requires legal opinion from case to case.

Regular review of the collection, storage and use of personal information

The information practices relating to the collection, storage and use of personal information will be reviewed by the Council every three (3) years. Any new program initiatives will be incorporated into the review process with a view to ascertaining whether or not those programs comply with the PPIPA and HRIPA.

Regular Review of Privacy Management Plan

Once the information practices are reviewed from time to time, the Privacy Management Plan will also be reviewed to ensure that the Plan is up to date.

Appendix 1

STATUTORY DECLARATION FOR ACCESS UNDER SECTION 57 OF THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998 TO A PUBLIC REGISTER HELD BY COUNCIL**STATUTORY DECLARATION
OATHS ACT, 1900, NINTH SCHEDULE**

I, the undersigned,(name of applicant)

of.....(address),

in the State of New South Wales, do solemnly and sincerely declare that:

I am.....(relationship (if any) to person inquired about)

I seek to know whether is on the public register of*

The purpose for which I seek this information is

The purpose for which the information is required is to

And I make this solemn declaration conscientiously believing the same to be true and by virtue of the Oaths Act 1900.

Declared at.....

in the said State this day of 200_
before me.

.....
before me:

Justice of the Peace/Solicitor

.....
Name to be printed

** Applicant to describe the relevant public register.*

Appendix 2

Privacy Notification Form - Section 10 (Post – Collection)

(Addressed to the person from whom information has been collected.)

The personal information that Council has collected from you is personal information for the purposes of the Privacy and Personal Information Protection Act 1998.

The intended recipients of the personal information are:

- ◆ officers within the Council;
- ◆ data service providers engaged by the Council from time to time;
- ◆ any other agent of the Council; and
- ◆ *(any other)*.

The supply of the information by you *is / is not* voluntary. If you cannot provide or do not wish to provide the information sought, the Council may

Council has collected this personal information from you in order to

.....

You may make application for access or amendment to information held by Council. You may also make a request that Council suppress your personal information from a public register. Council will consider any such application in accordance with the PPIPA.

Council* is to be regarded as the agency that holds the information.

Enquires concerning this matter can be addressed to

Signed.....

Dated.....

*Please state who holds or controls the information if not Council

Appendix 2a

Privacy Notification Form - Section 10 (Post – Collection from other source)

(Addressed to the person from whom information is about to be collected or has been collected.)

The personal information that Council is collecting from you is personal information for the purposes of the Privacy and Personal Information Protection Act 1998.

The intended recipients of the personal information are:

- ♦ officers within the Council;
- ♦ data service providers engaged by the Council from time to time;
- ♦ any other agent of the Council; and
- ♦ (any other).

The supply of the information by you is / is not voluntary. If you cannot provide or do not wish to provide the information sought, the Council may.....

Council is collecting this personal information from <other source name> about you in order to

You may make application for access or amendment to information held by Council. You may also make a request that Council suppress your personal information from a public register. Council will consider any such application in accordance with the PPIPA.

Council* is to be regarded as the agency that holds the information.

Enquires concerning this matter can be addressed to

Signed.....

Dated.....

Appendix 3

Privacy Notification Form - Section 10 (Pre –Collection)

(Addressed to the person from whom information is about to be collected or has been collected.)

The personal information that Council is collecting from you is personal information for the purposes of the Privacy and Personal Information Protection Act 1998 ("the Act").

The intended recipients of the personal information are:

- ♦ officers within the Council;
- ♦ data service providers engaged by the Council from time to time;
- ♦ any other agent of the Council; and
- ♦ *(any other)*.

The supply of the information by you *is / is not* voluntary. If you cannot provide or do not wish to provide the information sought, the Council may/will be unable to process your application.

Council is collecting this personal information from you in order to

.....

You may make application for access or amendment to information held by Council. You may also make a request that Council suppress your personal information from a public register. Council will consider any such application in accordance with the Act.

Council* is to be regarded as the agency that holds the information.

Enquires concerning this matter can be addressed to

Signed.....

Dated.....

*Please state who holds or controls the information if not Council

Appendix 4

**APPLICATION UNDER SECTION 13 OF THE PRIVACY AND PERSONAL INFORMATION
PROTECTION ACT 1998 –
TO DETERMINE WHETHER COUNCIL HOLDS PERSONAL INFORMATION ABOUT A
PERSON**

Personal information held by the Council

I, _____, of (address), hereby request the General Manager of Council
provide the following :

Does the Council hold personal information about me ? YES/NO

If so, what is the nature of that information?

.....
.....
.....

What is the main purpose for holding the information?

.....
.....
.....

Am I entitled to access the information? YES/NO

My address for response to this Application is:

.....
.....
.....

Note to applicants

Should you provide your address or any other contact details the Council will not record those details for any other purpose other than to respond to your application.

As an applicant, you have a right of access to personal information concerning yourself that is held by the Council under section 14 of the Privacy and Personal Information Protection Act 1998 ("the Act"). There is a separate application form to gain access.

The Council may refuse to process this application in part or in whole if:

- ◆ there is an exemption to section 13 of the Act; or
- ◆ a Code may restrict the operation of section 14.

Appendix 5

<p>APPLICATION UNDER SECTION 14 OF THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998 - FOR ACCESS TO APPLICANT'S PERSONAL INFORMATION</p> <p><u>Personal information held by Council</u></p> <p>I, (name).....</p> <p>of (address),</p> <p>hereby request that the Council provide me with:</p> <p>(a) access to all personal information held concerning myself; or (b) access to the following personal information only.....</p> <p><u>Note to applicants :</u></p> <p>As an applicant, you have a right of access to your personal information held by the Council under section 14 of the Privacy and Personal Information Protection Act 1998 ("the Act").</p> <p>You are entitled to have access without excessive delay or cost.</p> <p>Council may refuse to process your Application in part or in whole if:</p> <ul style="list-style-type: none">◆ the correct amount of fees has not been paid;◆ there is an exemption to section 14 of the Act; or◆ a Code of Practice may restrict disclosure. <p>Enquires concerning this application should be made to</p>

Appendix 6

<p align="center">APPLICATION UNDER SECTION 15 OF THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998 – FOR ALTERATION OF APPLICANT'S PERSONAL INFORMATION</p> <p><u>Personal Information held by Council</u> I, (name)..... of (address), hereby request the Council to alter personal information regarding myself in the following manner :</p> <p>I propose the following changes: </p> <p>The reasons for the changes are as follows : </p> <p>The documentary bases for those changes is as shown on the attached documents : </p> <p><u>Note to Applicants :</u> You have a right to request appropriate amendments are made (whether by way of corrections, deletions or additions) to ensure that the personal information held by the Council :</p> <p>(a) is accurate, and (b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.</p> <p>If Council is not prepared to amend the personal information in accordance with a request by you, Council must take such steps as are reasonable to attach to the information in such a manner as is capable of being read with the information, any statement provided by you.</p> <p>If your personal information is amended, you are entitled under the Privacy and Personal Information Protection Act 1998 ("the Act"), <u>if it is reasonably practicable</u>, to the have recipients of that information notified of the amendments made by Council.</p> <p>Council may refuse to process your application in part or in whole if:</p> <ul style="list-style-type: none"> ♦ there is an exemption to section 15 of the Act; or ♦ a Code of Practice may restrict alteration. <p>Enquires concerning this application should be made to</p>
--



COUNCIL POLICY:	Data Breach Response
Ref:	

Contact Officer	Director Corporate Services, Corporate Services
Approval Date	
Approval Authority	Council
Reviewed	Every four years
Amended / Reviewed	
Date of Next Review	

Overview

The Notifiable Data Breaches (NDB) scheme went into force on February 22, 2018, under the federal *Privacy Act 1988* (Privacy Act). Under the NDB program, organisations and individuals must notify impacted persons as well as the Office of the Australia Information Commissioner (OAIC) and Information and Privacy commission (IPC), NSW when a data breach is likely to result in substantial harm to an individual whose personal information has been compromised.

Along with the NDB program, the NSW Information and Privacy Commission must comply with the Commonwealth NDB scheme specifically in relation to breaches of tax file numbers (TFN). The introduction of the NSW Mandatory Notifiable Data Breach (MNDB) scheme aims to align with the Commonwealth NDB scheme and reduce inter-jurisdictional inconsistencies.

While the Commonwealth NDB scheme primarily targets Commonwealth government agencies and private sector organisations regulated by the APPs under the Privacy Act, there are provisions that also apply to NSW public sector agencies, especially regarding TFN breaches.

The Inverell Shire Council keeps records of individuals' personal information, including ratepayer, resident, and customer statistics and information. Additionally, the Council keeps track of employee and personal information. In order to plan, monitor, and manage the workforce, services, and properties throughout the Local Government Area (LGA), the Council gathers this data.

Given that the Council needs to use personal information to provide its services, Council must comply with the mandatory requirements of the Notifiable Data Breach scheme, which entails establishing a data breach notification protocol as required by the legislative changes set in November 2023, guiding the Council to exercise the utmost caution when handling personal information.

In the event that a data breach occurs, Council must abide by the scheme's notification requirements since failure to do so could subject Council to severe penalties under Australian law.

Scope

The purpose of this policy is to provide a procedure detailing the key actions and responsibilities to be followed in the event of a data breach incident. It makes use of the four crucial actions recommended by the OAIC and IPC for handling a data breach (see Appendix B).

The scope of this policy applies to all data held by Council in either a paper-based or electronic format and is applicable to all employees (including councilors, contractors, students, volunteers and agency personnel) as well as external organisations and contractors who have been granted access to Council's infrastructure, services and data.

This procedure supplements Inverell Shire Council's Privacy Management Plan.

Data Breach Management Plan

What is a Data Breach?

A data breach is an incident, in which personal or confidential information, or non-personal information that could be sensitive or commercial, is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen, or used by unauthorised individuals, whether accidentally or intentionally. Examples of data breaches include, but not limited to:

- A device with a customer's personal information is lost or stolen.
- A database with personal information is hacked.
- Unauthorised use, access to or modification of data or information systems.
- Personal information is mistakenly given to the wrong person.
- Unauthorised disclosure of classified material or personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted onto the IPC website without consent.

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

When do we know it has occurred?

Council may be made aware of a data breach through a complaint from a member of staff, a contractor, an impacted third party, or a report from another government department. A written request for an internal examination of a privacy complaint involving a data breach occurrence may also be sent to Council.

When does a breach become eligible for notification?

Affected persons, OAIC and IPC must be notified of a qualifying data breach under the Notifiable Data Breach (NDB) scheme.

A qualifying data breach happens when:

- Unauthorised access to, unauthorised disclosure of, or loss of personal information that a company or agency holds.
- Something that is likely to cause one or more people serious "harm".
- The company or agency hasn't been able to prevent the risk of serious harm with preventative measures.
- Government sector data has been exposed.
- Data breaches involving health records (within the meaning of the Health Records and Information Privacy Act 2002).

The following elements can be used to assess the "harm" produced by a breach and may be utilised to make a determination:

- Legal liability
- Financial loss
- Emotional wellbeing/loss
- Physical safety of the person/organisation
- Reputational damage
- Breach of secrecy provisions

An entity or agency that suspects an eligible data breach has occurred must analyse the situation as soon as possible to determine if it is likely to cause substantial harm to any individual.

NOTE: The relevant OAIC guidelines are available at <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches>; <https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-data-breaches-involving-tax-file-numbers> and provide further information on assessing an eligible breach.

Timeframe for assessing potential Data Breach

The Council is required to take all reasonable steps to complete the assessment within 30 calendar days of being aware of the qualifying data breach.

Where the Council is unable to reasonably complete an assessment within 30 days, the OAIC and IPC recommends that it document this so that it can demonstrate:

- That all reasonable steps were taken to complete the assessment within 30 days.
- The reasons for the delay.
- That the evaluation was reasonable and expeditious.

How to report a Data Breach?

A known or suspected data breach should be reported verbally or in writing to Manager Information Services as soon as possible, who will commence the response process.

Data Breach Response Process

1. Contain

- As soon as a suspected breach is reported, the Manager Information Services should gather the essential information and determine if a breach has occurred. If no breach is determined, complete a file note on the incident and advise the Director Corporate and Economic Services.
- If a breach occurred, complete the Data Breach Incident and Response Report - Part A (See Appendix A), notify the Director Corporate and Economic Services and keep any proof of the breach.
- Once the details of the incident have been gathered, the Manager Information Services should take the necessary steps to contain the breach (this may include coordinating with other staff members to ensure necessary steps/measures are put in place).
- Once a preliminary assessment of the level of risk posed by the breach (High, Medium, Low) has been established, notify the Response Team, and arrange a time to assess the breach.

2. Assess

- The Data Breach Response Team should evaluate the Manager Information Services preliminary evaluation and complete the Data Breach Incident and Response Report - Part B (See Appendix A).
- The following should be given special consideration because they will decide the implications for Council in terms of the notification process;
- Whether the violation is likely to cause serious harm to any affected parties
- Council may seek third-party help or advice from the NSW Information and Privacy Commission to provide an opinion or validate the Response Team's assessment.
- Any additional corrective actions identified by the Response Team to contain or mitigate the severity of the breach should be implemented.
- The assessment of the breach should be performed as soon as possible, but no later than 30 days after the breach is notified.

3. Notify

- After the Data Breach Incident and Response Report (See Appendix A) has been completed and reviewed by the Response Team, and it is determined that Council is legally required to provide notification of the incident, notification is expected to occur within 72 hours of the assessment.
- If required, the OAIC and the NSW Information and Privacy Commission should be notified.
 - OAIC - <https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/>
 - NSW Information and Privacy Commission.
<https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification>
- Council must then notify individuals at risk of serious harm either;
 - directly notify only those individuals at risk of serious harm, or
 - directly notify all individuals whose data was breached,
- If the individuals affected are not known or can't be identified, then Council will;
 - Publicise the statement more broadly.
- The Manager Administrative and Marketing Services must be alerted in order to write a Media Statement in response to the data breach, if necessary.
 - Data Breach Incident and Response Report - Part B (See Appendix A) contains guidelines for notifying a breach. This should be used as a guideline when communicating breaches with individuals and in general.

4. Review

- Following the assessment of the incident and notification, the Manager Information Services should conduct a review within 14 days to identify any actions required to prevent further breaches, which should be tabled at the Management Team Meeting and include:
 - Recommended changes to system and physical security
 - Recommended suggestions for revisions to any Council policies or processes.
 - Staff training and education should be revised or changed.

5. Prevent

- Once immediate steps have been taken to mitigate the risks associated with a breach, the Council must take the time to investigate the cause of the breach.
- The Management Team must be briefed on the outcome of the investigation, including recommendations:
 - To make appropriate changes to policies and procedures if necessary.
 - Revise staff training practices if necessary.
 - Update this Response Plan if necessary.

Roles & Responsibilities

Staff in the following positions will typically make up the Data Breach Response Team:

Position	Responsibilities
General Manager (High Risk Only)	<ul style="list-style-type: none"> General advice
Director Corporate and Economic Services	<ul style="list-style-type: none"> General governance and advice Process oversight, quality assurance General advice and direct linkage to executives
Manager Information Services	<ul style="list-style-type: none"> Compliance and records management advice and coordination of preliminary assessment and response team Provide advice around application-level data/information security Provide advice around technical/IT infrastructure security
Manager Administrative and Marketing Services	<ul style="list-style-type: none"> Communications advice
Legal Counsel (third party)	<ul style="list-style-type: none"> Legal advice

The Response Team may also seek advice from 3rd Party privacy specialists or the NSW Information and Privacy Commission if deemed necessary as part of the assessment process.

References

This Data Breach Response Policy is based on the OAIC's Data breach notification: a guide to dealing with information security breaches, and the IPC Data Brach Guidance for NSW Agencies.

In the case of a data breach, the Response Team should refer to the Guide since it contains additional information that may be useful to the Response Team.

- <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>
- <https://www.ipc.nsw.gov.au/resources/ipc-data-breach-notification-form>
- <https://www.ipc.nsw.gov.au/data-breach-guidance-nsw-agencies>
- <https://www.ipc.nsw.gov.au/fact-sheet-notification-affected-individuals-data-breach>
- <https://www.ipc.nsw.gov.au/fact-sheet-nsw-public-sector-agencies-and-data-breaches-involving-tax-file-numbers>
- <https://www.ipc.nsw.gov.au/fact-sheet-mandatory-notification-data-breach-scheme-exemptions-notification-requirements>

Related Documents and Council Policy

- Inverell Shire Council Privacy Management Plan.
- Information and Privacy Commission Website.
- Office of the Australian Information Commissioner Website.

Related Legislation

- Privacy Act 1988 (Privacy Act).
- Privacy and Personal Information Protection Act 1998

Appendix

Appendix A – Data Breach Incident Report

Part A – Data Breach Incident Report

To be completed by the Manager Information Services (or his/her representative) on receipt of a breach report.

Name/Position:	Date:
When, where and how did the breach occur?	
Who and how was the breach discovered?	
When was the breach first reported to the Manager Governance?	
How would you classify the breach? <ul style="list-style-type: none"> • Unauthorised access • Unauthorised disclosure • Loss • Alteration • Destruction of personal information 	What information/data has been compromised? <ul style="list-style-type: none"> • Financial details • Tax File Number • Identity Information • Contact Information • Health Information • Other
What parties have been affected by the breach?	
Steps taken to immediately contain the breach?	
Do any external parties been notified about the breach? E.g. The OAIC, NSW Information and Privacy Commission, Police, Insurance providers, credit card companies etc.	
Preliminary Assessment of risk posed by the data breach? <ul style="list-style-type: none"> • High Risk (established or suspected) = likely to result in serious harm to affected individual/s or organization • Moderate Risk • Low Risk 	

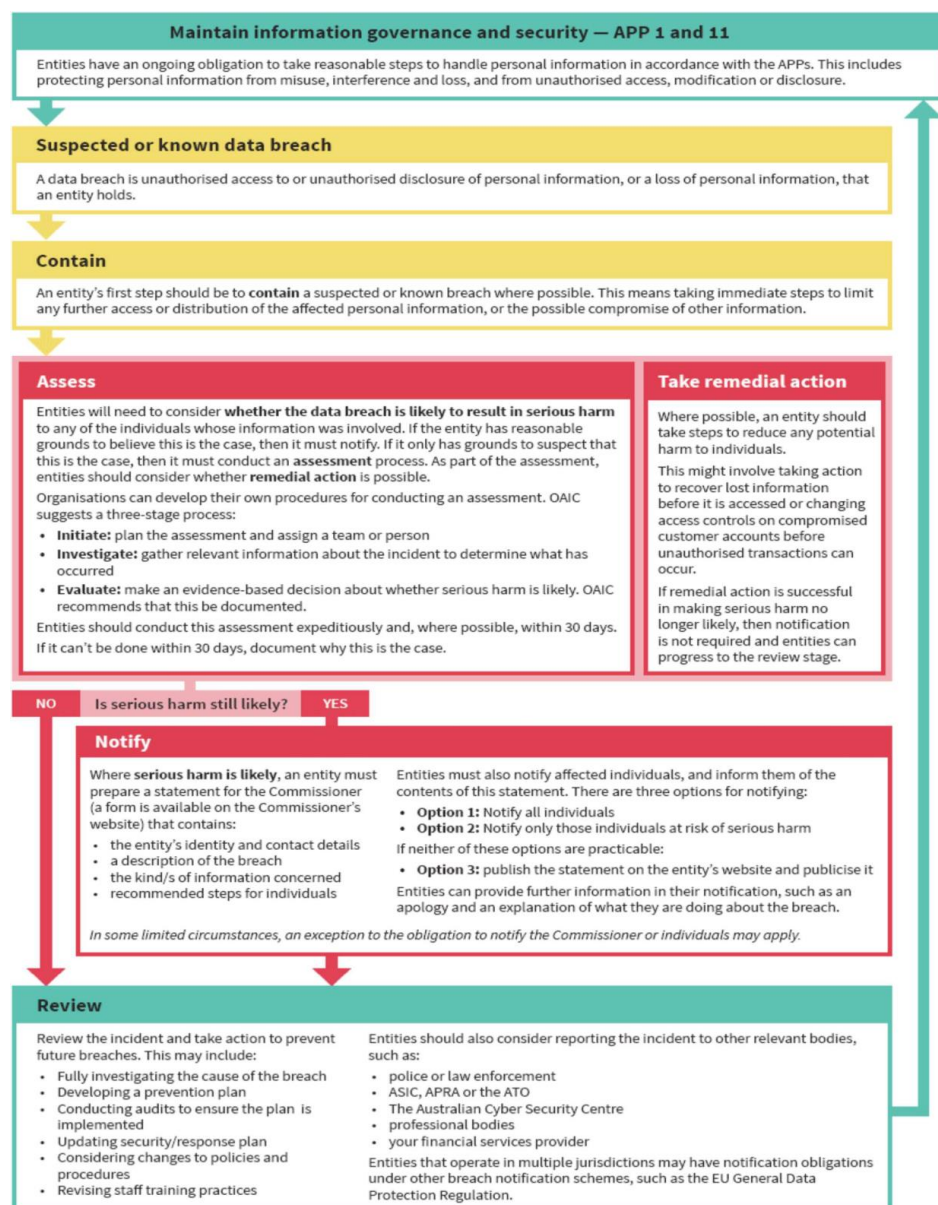
Part B – Data Breach Response Report

To be completed by the Manager Information Services at completion of the Response Team's assessment meeting.

Name/Position:	Date:
List the response team members	
Listing of preliminary steps that have been taken to contain the breach	
Any further steps identified to minimise the impact on affected individuals or organisations?	
Validation of risk posed by the data breach? High Risk (established or suspected) = likely to result in serious harm to affected individual/s or organisation <ul style="list-style-type: none"> • Moderate Risk • Low Risk 	
Confirmation of notification required NDB Eligible data breach – mandatory disclosure (high risk) Council elected voluntary disclosure (low or medium risk) GDPR data breach – mandatory disclosure required within 72 hours (high, medium or low risk)	
Agencies notified <ul style="list-style-type: none"> • OAIC • NSW Information and Privacy Commission 	
Confirmation of Notification Approach <ul style="list-style-type: none"> • Directly notify only those individuals at risk of serious harm, or • Directly notify all individuals whose data was breached, • Publicise the statement more broadly. Please specify whether notification is to occur via phone, letter, email or in person.	
Next steps for Review phase	

Appendix B – OAIC's – Four key steps to responding to data breaches

The following diagram provides an overview of a typical data breach response, including the requirements of the NDB scheme. This diagram is a summary and should be read with reference to the more detailed resources listed above.



INVERELL SHIRE COUNCIL'S Eligible Data Breach Incident Register								
Note: Inverell Shire Council's Incident Data Breach Notification Register is in compliance with the <i>Privacy and Personal Information Protection Act 1998 (PPIP Act)</i> which established the NSW Mandatory Notification of Data Breach (MNDB) scheme. The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to Agencies must establish and maintain an internal register for eligible data breaches. Each eligible data breach must be entered on the register, with the following information included for each entry where practicable as recommended by the IPC (Information and Privacy Commission NSW).								
Breach Notification Date	Breach Notified By	Breach Notified To	Type of Breach Eg unauthorised access, unauthorised disclosure or loss of information	How Breach Occurred	Type of Personal Information Impacted by Breach	Action Taken or Planned to mitigate harm done by the Breach	Action taken to prevent future breaches	Estimated cost of the breach

INVERELL SHIRE COUNCIL'S PUBLIC DATA BREACH NOTIFICATION REGISTER									
<div>Note: Inverell Shire Council's Public Data Breach Notification Register is in compliance with the <i>Privacy and Personal Information Protection Act 1998 (PPIP Act)</i> which established the NSW Mandatory Notification of Data Breach (MNDB) scheme. The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to notify affected individuals of eligible data breaches. This register will be updated as required and information contained within will remain available for at least 12 months after the date of the data breach public notification, as recommended by the IPC (Information and Privacy Commission NSW).</div>									
Date of Breach	Description of Breach	Type of Breach Eg unauthorised access, unauthorised disclosure or loss of information	How Breach Occurred	Type of Personal Information Impacted by Breach	Action Taken or Planned to ensure Personal Information is Secure and to Mitigate harm to Individuals	Steps Individuals are Recommended to Take in Response to the Breach	Date of Public Notification	For Further Assistance Contact	Link to Full Public Notification

4.4 REFERRAL OF CONFIDENTIAL MATTERS**File Number:** S24.11.4 / 23/33129**Author:** Kristy Paton, Corporate Support Officer - Publishing**SUMMARY:**

Referral of Confidential Report.

RECOMMENDATION:

That the Committee refer the items to Closed (Public excluded) meeting of the Committee and that the press and members of the public be asked to leave the chambers whilst the Committee considers the following items:

Item: 6.1 Outstanding Debtor Account - 215057-1

Authority: Section 10A (2) (a) Personnel matters concerning particular individuals (other than councillors).

COMMENTARY:

In accordance with the provisions of Section 9 (2A) *Local Government Act 1993*, the General Manager is of the opinion that consideration of the following item(s) is likely to take place when the meeting is closed to the public.

Item: Outstanding Debtor Account - 215057-1

Description: A debt is owed to Council for clean-up costs associated with a property in the village of Tingha. The debt to date including legal fees and excluding interest is \$41,785.48.

A proposal has been submitted to Council for consideration. The purpose of this report is to consider the proposal, decide whether or not to continue legal action or write off the debt.

Reason: Personnel matters concerning particular individuals (other than councillors) (s. 10A (2) (a) *Local Government Act 1993*).

5 GOVERNANCE REPORTS

5.1 RISK MANAGEMENT FRAMEWORK

File Number: S27.8.1 / 23/33084

Author: Paul Pay, Director Corporate and Economic Services

SUMMARY:

The Audit Risk and Improvement Committee (ARIC) have reviewed Council's Risk Management Framework and the Committee is asked to endorse the recommended changes.

RECOMMENDATION:

That the Committee recommend to Council that the Risk Management Framework be adopted.

COMMENTARY:

In accordance with the Audit Risk and Improvement Committee (ARIC) Charter, ARIC has reviewed the Risk Management Framework at its September 2023 meeting.

The Risk Management Framework outlines Council's organisational risk management approach. The framework provides the structure and tools that will facilitate the use of a consistent risk management process whenever decisions are being made in Council. This framework must be applied consistently across all projects, functions, processes and activities at all levels of Council to ensure resources used to treat risks are available and applied efficiently and effectively.

ARIC have only recommended one change to the current Risk Management Framework, a change to the definition of "Controls" as shown below.

Current "Controls" definition

A mechanism put in place to respond to the impact in the event of a risk occurring and reduce the resulting impact e.g. business continuity plan.

Recommended "Controls" definition

Risk Control is a way for organisations to mitigate risk by implementing operational processes. For example, a Council might control the risk of equipment failure by preforming maintenance according to a set schedule.

A copy of the revised Risk Management Framework is attached for your reference.

RISK ASSESSMENT:

Nil

POLICY IMPLICATIONS:

Nil

CHIEF FINANCIAL OFFICERS COMMENT:

Nil

LEGAL IMPLICATIONS:

Nil

ATTACHMENTS:

1. Risk Management Framework [↓](#)



Inverell Shire Council

Risk Management Framework



Document Control Page

Trim Reference: 17/29799

Version	Date	Author	Approved / Authorised	Approved Date	Revision Comment
1.0	September 2017	Mathew de Witt			
2.0	February 2020	Sally Williams	Scott Norman		Revised as per request by Audit Risk & Improvement Committee.
3.0	February 2023	Paul Pay	Council		Revised to include new Risk Appetite Statements
4.0	October 2023	Paul Pay	Council		Framework reviewed and updated by ARIC September 2023 .



Table of Contents

Purpose.....	4
Definitions.....	5
Risk Management Framework.....	7
Risk Appetite.....	7
Risk Appetite Statement.....	8
Risk Management Process Overview.....	9
Risk Assessment Process.....	10
Assessing Inherent Risk.....	11
Identification and Assessment of Controls.....	13
Evaluating Residual Risk.....	14
Develop and Implement Strategies.....	15
Monitoring Strategies.....	16
Risk Reporting and Escalation.....	16
Monitoring and Reporting Flowchart.....	17
Communication and Consultation.....	18
Accountability.....	19
Implementation.....	20
Review.....	20
References.....	20



Purpose

The purpose of this document is to outline Council's organisational risk management approach.

Risk is the effect of uncertainty on achieving Inverell Shire Council's (Council) objectives.

Council undertakes risk management processes to understand the risks it faces and to manage and mitigate uncertainty to a tolerable level. This procedure details the system, including templates and terminology used by Council to manage risk. Effective risk management involves all staff and applies to all Council activities.

Successful management of risk can:

- Improve organisational performance and increase organisational resilience;
- Reduce foreseeable threats to a level that Council is willing to accept; and
- Enable Council to maximise opportunities that may present themselves.

An effective risk management process is a foundation of good corporate governance, which supports management in the achievement of Council's Community Strategic Plan and Operational plan objectives and ensures Council remains resilient and contemporary moving into the future.

Scope

This Risk Management Framework provides the structure and tools that will facilitate the use of a consistent risk management process whenever decisions are being made in Council. This framework must be applied consistently across all projects, functions, processes and activities at all levels of Council to ensure resources used to treat risks are available and applied efficiently and effectively.

Council's General Manager is ultimately accountable for the decisions made in the operations of Council and therefore is required to know that important issues are being managed and that set objectives will be achieved. Council's Director Corporate and Economic Services and Director Civil and Environmental Services receive information on Council's management of risk through reporting provided by the Audit, Risk & Improvement Committee and Risk Management Committee. This information is then made available to the General Manager and Councillors.

In addition, it is a requirement under the NSW Local Government Act that Council have a Risk Management Framework in place. To meet these expectations and as a standard of good governance, Council has introduced a system of risk management planning and monitoring, which is based on the standard AS/NZS ISO31000:2018 Risk Management-Principles and Guidelines.



Definitions

Terms	Definitions
Context	Describes the goals, objectives and depth of analysis for the area of review. It considers the external and internal environment in which Council seeks to achieve its objectives.
Controls	Risk Control is a way for organisations to mitigate risk by implementing operational processes. For example, a Council might control the risk of equipment failure by performing maintenance according to a set schedule.
Control owner	Person responsible for implementing selected control measures. For example ensuring playgrounds receive regular documented inspections.
Risk	The effect of uncertainty on achieving Council's objectives. Risk is measured in terms of likelihood and consequence.
Inherent Risk	The level of risk that exists prior to control measures being introduced or applied, or the level of risk that exists if controls and risk treatments were removed or not applied.
Residual Risk	The level of risk remaining after control measures have been implemented.
Risk Event	An occurrence or change in a particular set of circumstances.
Risk Assessment	A systematic process of risk identification analysis and evaluation.
Risk Likelihood	The chance of an event occurring.
Risk Consequence	The outcome of an event expressed qualitatively or quantitatively, affecting Council objectives. There may be a range of possible outcomes associated with an event; these could have a positive or negative impact on objectives.
Risk Level	Defined by applying the likelihood and consequence of an event to Council's endorsed risk matrix.
Risk Management	The culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects. Risk management will provide greater assurance that Council is achieving its objectives by minimising threats and seizing opportunities.

Administration Centre, 144 Otho Street (PO Box 138), Inverell NSW 2360

Ph: 02 67 288 288 Fax: 02 67 288 277

DX 6159

www.inverell.nsw.gov.au

Page | 5



Definitions continued

Terms	Definitions
Risk Management Plan	<p>Inverell Shire Council's Corporate Risk Register Trim reference 17/32613 which:</p> <ul style="list-style-type: none"> • identifies risks; • identifies possible impact; • assesses their likelihood and consequence of occurrence; • identifies inherent level of risk; • identifies controls and management strategies; • makes an assessment of the effectiveness controls; • assesses the residual; • identifies responsible person or control owner; and • sets standard for the monitoring of identified risk
Responsible Person	The position with accountability and authority to manage a risk. For example, ensuring resources and training are available for the control owner to conduct regular playground inspections
Risk Tolerance/Appetite	The level of risk Council is willing to accept or pursue in order to achieve objectives.



Risk Management Framework

The Risk Management Framework within Council operates in line with Council's Risk Management Policy Trim reference 17/29786 and each Destination as set out in Council's Delivery Plan.

Each Strategy which falls under its relative destination incorporates both Key and Operational risks to the organisation.

Corporate Risks are those risks that can impact the achievement of Council's objectives and corporate strategy.

Operational risks are those risks that occur as part of Council undertaking its business activities and often feed into a Key Risk, for example the risks associated with the achievement of project objectives.

As part of this framework, departments within Council will develop specific policies or procedures for managing risk in an area of operation. For example, Project Management, Work Health and Safety or Asset Management. Specific procedures should only be developed where this procedure does not fully cover the requirement or where further explanation is necessary.

Council's "Footpaths Management Procedure" is an example where an additional procedure was required to be developed in order to specifically outline and document how Council manages risks associated with footpaths in the Central Business District.

Risk Appetite

Risk appetite is the amount and type of risk that an organisation is willing to accept in order to meet its strategic objectives, incorporating the internal and external capabilities available to manage those risks. Without clearly defined and measurable tolerances Council is unable to make sound business decisions based on the level of risk it presents.

The diverse range of business activities undertaken by Local Government provides significant challenges in defining Council's risk appetite. Clear articulation of the context in which risks are being assessed is essential to ensure the best potential controls are selected and implemented and assist Council in making sound decisions.

Council's risk appetite statement is summarised on the following page. See appendix 1 for full document.



Council Risk Appetite Statement

Financial

1. Council has no appetite for decisions that have a significant negative impact on Council's long term financial sustainability.

Legal and Regulatory

2. Council has no appetite for non-compliance with legal, professional and regulatory requirements.

Human Resources

3. Council has no appetite for compromising staff safety and welfare.
4. Council has a low appetite for risks arising from inadequately trained staff or failed internal processes.

Operational

5. Council has a low appetite for system failures or information and data security breaches.
6. Council has a medium appetite for operational risks associated with the implementation of change and key strategic plans.
7. Council has no appetite for internal fraud, collusion, theft and/or associated reputational risk.
8. Council has a low appetite for operational risks arising from failure to meet customer commitments and/or suitability of advice.
9. Council a low appetite for third party partner (contractors) failure.
10. Council has considerable appetite for improvements to service delivery.
11. Council has considerable appetite for improved efficiency of Council operations.

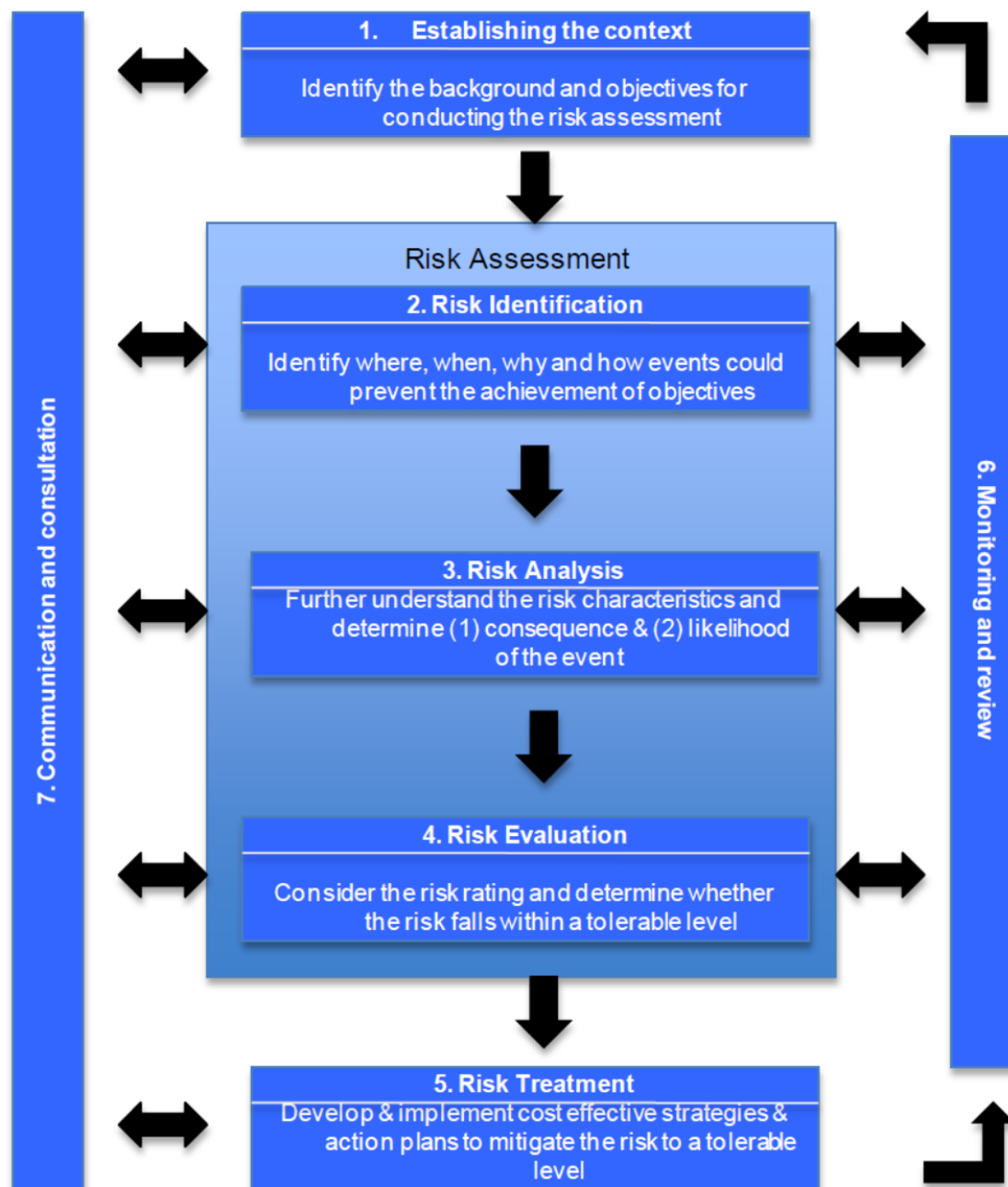
Environmental

12. Council has considerable appetite for decisions that promote ecologically sustainable development.



Risk Management Process Overview

Consistent with the AS/NZS ISO31000:2018





Risk Assessment Process

Detailed below are the suggested steps that provide guidance for undertaking a risk assessment. The process does not necessarily have to be undertaken in sequence and when reviewing action plans some steps may not be required.

Risk Assessments should be undertaken by people who have detailed knowledge of the functional area being assessed. Council's Audit, Risk & Improvement Committee, persons with overall responsibility and where required, with the assistance of Council's WHS & Risk Coordinator.

Risk Assessments are imperative and are designed to direct attention to certain areas rather than be a precise quantification of any impact on Council. For instance a risk that has minor impact, is unlikely to occur and is effectively controlled would not require any further treatment actions. Consistent risk assessment by risk owners are important to ensure any risks are effectively identified and controlled where possible.

Step 1 – Establish the Context

Identify the background and objectives for conducting the risk assessment

The scope of the activity or decision, or parts of Council to which this risk management process is to be applied should be established and the objective of that process or activity clearly understood, including its relationship to the overall objectives of Council.

The assessment should be undertaken with consideration of the need to balance costs, benefits and opportunities. Inclusions, exclusions, assumptions and limitations should be articulated to ensure that all parties have a shared understanding of the area under review.

Without context, the type or level of resources that should be assigned to manage the risk cannot be determined. For example, understanding Community expectations will influence the assessment of the consequences of certain events.

Step 2 – Risk Identification

Identify where, when, why and how events could prevent the achievement of objectives

Identify the risk source or uncertainty in achieving the objective, the cause and potential consequence. Risks may be identified from a review of hazards or vulnerabilities, or by the review of processes or functions and where they might impact the delivery of objectives.

Risk management is cyclical and lists of risks will evolve over time.

Council's Corporate Risk Register can be found in Trim; record 17/29370.



Step 3 – Risk Analysis

Further understand the risk characteristics and determine the consequence & the likelihood of the event.

While there is a subjective element to the assessment of risk, there must be a basis behind the assessment. Assumptions should be articulated and risk assessments documented to ensure accountability and evidence of due diligence.

Assessing Inherent Risk

Identify the risk and consequence inherent in the area and objective Council is aiming to achieve. At this stage the risk is assessed without the application of any control measures so is rated at the worst-case scenario level.

When determining likelihood it is important to consider the frequency and exposure to the risk in the overall context. For example, a daily action/task/event versus annual or quarterly. The higher or longer the exposure, the more likely the event is to occur.

Likelihood Ratings

Level	Description
Rare	The event may occur but only in exceptional circumstances; No past event history; More than 25 years.
Unlikely	The event could occur at some time; no past event history; within 10-25 years.
Possible	The event might occur at some time; No past event history; Once every 10 years.
Likely	The event is likely to occur in most circumstances; Some recurring past event history; Once per year.
Almost Certain	The event is expected to occur in most circumstances; There has been frequent past events; More than once per year.

Consequence Ratings

Consequence Categories			Consequence Ratings				
What could be the impact on Council and/or the project if the risk occurs?			How severe could the consequences be if the risk occurs				
			Insignificant	Minor	Moderate	Major	Catastrophic
ORGANISATION	Financial	Risks that have a financial impact on the organisation (revenue, expenses, assets, liabilities, reserves)	Up to \$10,000 loss	Up to \$100,000 loss	Up to \$250,000 loss	Up to 1 Million dollar loss	Over 10 Million dollar loss
	People	Risks that impact the safety and wellbeing of staff and the community	Insignificant injury, no first aid required; no impact on staff morale/performance/culture	Minor injury; first aid required; minor impact on staff morale/performance in single business area of organisation	Medical attention; several days leave; substantial impact on staff morale/performance in some business areas of organisation	Long term illness or injury; extensive leave required; significant impact on staff morale/performance across multiple areas of organisation	Could kill or cause permanent disability or ill health; major ongoing impact on staff morale/performance across entire organisation
	Service Delivery	Risks that impact the ability to deliver internal/external services and/or the expected level of service delivery	Isolated, minimal impact on service delivery (<1 day); no/minimal inconvenience to customers	Minor impact on service delivery (1 day - 2 weeks); some inconvenience to customers; isolated customer complaints	Substantial impact on service delivery (2 weeks - 1 month); substantial inconvenience to customers; higher than normal customer complaints	Significant impact / disruption to key service delivery (1 month – 2 months); significant inconvenience for customers; consistent high level of customer complaints	Extensive impact/disruption to key service delivery (> 2 months); major inconvenience for customers; systematic / serious customer complaints; potential threat to viability of organisation
	Compliance	Risks that impact compliance with legislation and regulatory requirements	Warning or issue of improvement notice; minor fine/penalty	Minor breach of legal obligations; adverse finding; minor fine/penalty	Substantial breach of legal obligations; adverse finding; substantial fine/penalty	Significant breach of legal obligations; adverse finding; significant fine/penalty	Major breach of legal obligations; adverse finding against individuals and/or the organisation; imprisonment; dismissal of Council; major fine/penalty
	Environmental	Risks that impact the natural environment	Insignificant, immediately reversible impacts on the environment	Limited short to medium term, quickly reversible impacts on the environment	Potentially significant medium term reversible impacts on the environment	Severe, medium to long term potentially irreversible impacts on the environment	Critical, long term irreversible impacts on the environment
	Reputation	Risks that impact Council's reputation with the community, media and government	Possibly some concern / enquiries from the community; no media / government attention	Minor unfavourable local media attention; minimal community and local government concern	Adverse short-term local/state media attention; increased community concern / criticism; some local / state government concern	Intense community and national media scrutiny; medium term loss of trust within factions of the community; adverse state government enquiry /intervention	Sustained adverse national media attention; complete and ongoing loss of community trust; major adverse state government action / loss of support
	Information Technology	Risks that impact Councils records, privacy of information or business continuity.	inaccurate data entry	Minor system issue resulting in under 2hrs lost system availability	Moderate system issue resulting in loss of system availability in excess of one day	Major system issue resulting in lengthy loss of system availability. Virus attack.	Complete system failure. Hacking event, substantial loss of data, sensitive Council information obtained and leaked.
PROJECTS	Project Budget	Risks that impact the ability to deliver project outcomes within budget	Slight impact on budget, manageable within funding	Marginal budget over-run, within management reserve	Substantial budget over-run outside any contingency reserve, may require extra resources	Critical budget over-run requiring additional funds	Major impact on the project's viability and may lead to cancellation
	Project Timeframes	Risks that impact the ability to deliver project outcomes within timeframe	Negligible impact on milestones, manageable within resources	Marginal impact on milestones, manageable within resources	Substantial impact on milestones and major activities, may not affect implementation date	Critical impact on milestones and major activities, requiring re-base lining of implementation date	Major over-run affecting many milestones. May lead to cancellation / inability to deliver services to plan.

Risk Matrix

		Consequence				
Likelihood		Insignificant	Minor	Moderate	Major	Catastrophic
	Almost Certain	Medium	High	High	Extreme	Extreme
	Likely	Medium	Medium	High	High	Extreme
	Possible	Low	Medium	High	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Medium	Medium	High

Identification and Assessment of Controls

As shown in the above matrix, risks are rated on a scale from low to extreme. Generally no further action is required for Low inherent risks, except to record and monitor them at least annually or whenever circumstances change, whichever comes first. This process is performed as Low risks can change in significance. In some instances low risks may be subject to excessive controls and this should be reviewed to ensure the appropriate balance of cost/benefit for risk and controls is in place. Too many or inefficient controls can also impact on Council's ability to meet objectives and may need to be removed.

For inherent risks rated other than low, determine what management strategies and/or controls are already in place to address the risks and determine suitability. The type of control utilised should be dependent on the risk itself and the cost/benefit obtained from introducing such controls, and how effective they are. If controls are costly they may not be the most efficient way to treat the risk as the risk reduction may not justify the cost of control.

When new controls need to be implemented, ensure the "Responsible Person" and the "Control Owner" is consulted. This not only provides the opportunity for expertise in the control area to be applied but also ensures strong communication lines and suitable implementation.



The table below provides guidance in determining controls suitability.

Control Suitability	Qualification of the Effectiveness of Controls
Ineffective	The controls that have been applied are not adequate in treating the risk.
Partial	The controls that have been applied go part of the way to treat the risk or impact.
Effective	The controls that have been applied are value for money to treat the risk or impact.
Excessive	The controls that have been applied are more than necessary to treat the risk and do not provide appropriate cost/benefit return.

Assessing Residual Risk

Once new or additional controls have been decided, the risk assessment process must be undertaken again to reevaluate the level of risk. Residual risks should never be higher than the inherent level.

Step 4 – Risk Evaluation

Evaluating Residual Risk

Once risk assessment of residual risk is undertaken, Council must decide whether the new risk rating falls within a tolerable level.

As a general rule, if the residual risk assessment results in either High or Extreme levels, then reviewed or additional controls should be identified and implemented where they are cost effective.

For Medium level residual risk levels, management should consider whether controls or further treatment actions are necessary and/or cost effective. No further action is generally required for low inherent or residual risks, except to record and monitor them at least annually or whenever circumstances change, whichever comes first.

For all risks the following risk treatments should be considered:

Acceptance - where the level of risk is at a level acceptable to Council. This generally occurs where the risk is low or at the point where the cost of further treatment is greater than the benefit derived.



Avoidance - refusing to accept the risk if it cannot be lowered by ceasing the activity where the risk occurs. This may not be the best alternative as a totally risk averse organisation will not grow and will generate a very low rate of return. In terms of Council, the growth would be in terms of asset provisioning and service delivery to the community

Reduction - reducing the likelihood and/or consequence if it is feasible and cost effective.

Transference - moving all or some of the risk to a third party. Transference of a risk does not mean the risk is entirely transferred but generally it is a partial transference through insurance coverage/contractual arrangements or some other means.

Increasing - where the level of risk is assessed as too low and is inhibiting Council's ability to achieve its objectives or the costs of controls do not match the benefits achieved.

Step 5 – Risk Treatments

Develop and Implement cost effective strategies and action plans to mitigate risk in line with Council's Risk Appetite.

When choosing a treatment action, the responsible person should also consider the cost of ongoing efforts and maintenance to ensure long-term viability. Sometimes a control with a high initial cost (e.g. an engineering solution) can be more cost effective in the long term than one with a low initial cost that needs high levels of effort or ongoing maintenance (e.g. the development of procedures with associated training, supervision and enforcement).

A determination should be made as to what further treatment actions will be taken to mitigate the risk to a tolerable level. Treatments should be actioned in accordance with risk rating action timeframes.

Extreme Risk - Immediate action is required or contingency plans implemented to address any operational issues. A plan should then be put in place within one month to manage the residual risk to an acceptable level.

High Risk - Immediate response is required or contingency plans implemented to address any operational issues. A cost effective plan should then be put in place within three months to manage the residual risk to an acceptable level.

Medium Risk - Monitor and attempt to reduce further as resources permit. Medium risks will generally be considered at a level that Council can accept.

Low Risk - Monitor and attempt to eliminate if possible as resources permit. Low Risks will generally be considered at a level that Council can accept.



Step 6 – Monitor and review

Monitoring Risk Management Strategies

Monitoring identified risks and control actions regularly is imperative in ensuring risks remain within the tolerable level and that mitigation strategies have been implemented, are effective and documented in Council's record system Trim.

Council's Corporate Risk Register is to be reviewed annually by the Audit, Risk & Improvement Committee and must include:

- a reassessment of the inherent risk based on changes in the internal and external environment;
- assessment of any emerging risks; and
- assessment of the effectiveness and efficiency in the application of controls and new treatment actions.

The review and subsequent assessment should be used for planning purposes as well as a management tool to direct resources and effort moving forward.

Risk Reporting and Escalation

Residual risks are to be actioned in accordance with Council's Risk Action Timeframes and nominated responsible person.

When a risk is identified it should be notified/escalated, based on its residual risk rating to the appropriate level of management. That manager should then assess whether the risk is mitigated to a level that is within Council's risk appetite.

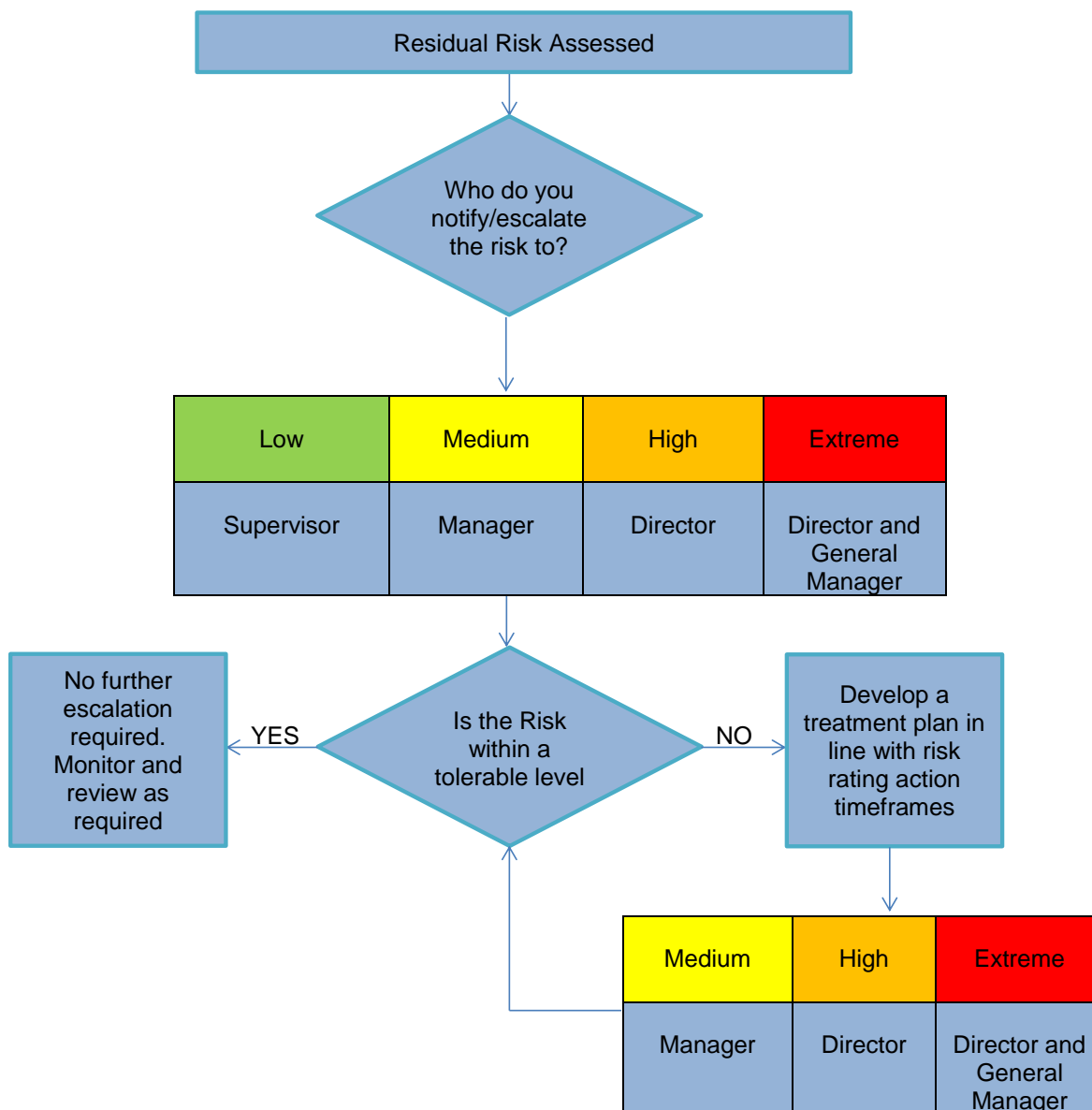
If the risk is within a range that is tolerable to Council, then the risk is accepted, included in Council's risk register and periodically monitored for any changes in the risk level.

If the risk is not considered to be within Council's appetite, then the risk should be recorded, treatment plans developed, implemented and monitored.

Monitoring should identify when risk levels increase due to changes in the environment or when controls are ineffective. If risk ratings increase then those risks should be escalated in accordance with the flowchart below. Risk or control owners should undertake a review of the residual risk when treatment actions are implemented to assess whether the action was effective.



Monitoring and Reporting Flow Chart





Step 7 – Communication and Consultation

Communication and consultation should take place during all stages of the risk management process. Internal and external stakeholders should be consulted to ensure that:

- the context in which Council operates is fully understood;
- the interests of stakeholders are understood and considered;
- all risks are identified;
- different areas of expertise are drawn on when analysing and evaluating risks and different views are considered; and
- endorsement and support for risk treatment plans is secured.

Both internal and external stakeholders will be interested in information on how Council is managing its risks. Different stakeholders will have different information needs, which influences the level and content of reporting in relation to risks.

Effective communication and consultation should take place to ensure that those accountable for implementing the risk management process and treatment actions across the organisation understand the basis on which decisions are made, and the reasons why particular actions are required.



Accountability

Guidelines under section 23A of the *Local Government Act 1993* state the following roles and responsibilities in the lines of reporting for risk management.

Role	Responsibilities
Councillors	Councillors make decisions on budgets, projects and have a major impact on goals that may have been set. Councillors must be aware of the risks associated with the decisions they make. Councillors also have an impact on how ratepayers perceive the organisation and its effectiveness.
General Manager	Council's General Manager has overall responsibility regarding the organisations operational management of risk
Chief Audit Executive (Director Corporate & Economic Services)	To ensure the functionality of Council's Audit, Risk & Improvement Committee.
Audit, Risk & Improvement Committee	The Audit, Risk & Improvement Committee is responsible for the oversight of the risk management process across Council. This includes advising the council regarding the Risk Management Framework and policy and monitoring and reviewing risk management effectiveness.
Directors	Ensuring resources are provided to implement required risk mitigation strategies and reporting to the Audit, Risk & Improvement Committee, and General Manager where required.
Managers	Assessing risk, coordinating implementation of risk controls and reporting to Directors where required. Monitoring and reviewing.
Supervisors	Assisting Manager in implementing risk controls
General Staff	Ensure all procedures are followed and reporting any identified risks to Supervisor or Manager.



Implementation

This framework will be implemented and supported through:

- communication with Councillors;
- communication with Council's General Manager and Directors;
- communication with Council's Audit, Risk and Improvement Committee;
- communication with managers and supervisors; and
- ongoing training and continual improvement.

Review

This framework will be reviewed as required, such as changes in legislation or risk management standards. Review will be undertaken by Council's Audit, Risk & Improvement Committee in consultation with Council Directors and General Manager.

References

AS/NZS ISO31000:2018 Risk Management-Principles and Guidelines

ISC Corporate Risk Register

ISC Audit, Risk & Improvement Committee Charter.

Guidelines under section 23A of the Local Government Act 1993 – Internal Audit Guidelines – September 2010 – Office of Local Government – Retrieved from <https://www.olg.nsw.gov.au/sites/default/files/Internal-Audit-Guidelines-September-2010.pdf>

Appendices

Appendix 1 – ISC Risk Appetite Statement



**statewide
mutual.**



RISK APPETITE STATEMENTS

Inverell Shire Council

Version: 1.0 | 15 December 2022



DOCUMENT CONTROL PAGE

Version	Date	Author	Approved / Authorised	Approved Date	Revision Comment
1.0	15 December 2023	Craig Hutley Principal, Strategic Risk, Marsh Advisory	Council	22 February 2023	Resolution 2023/21



TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
RISK APPETITE SUMMARY	4
RISK APPETITE STATEMENTS	5
CONCLUSION	8
CONTACTS	8



EXECUTIVE SUMMARY

Risk Appetite is an articulation of an organisation's willingness to take, retain or accept risk and, because it operates at strategic and operational levels, it is an integral part of any risk management capability. In order to influence strategies and objectives it should be considered and reviewed during Strategic Planning. Additionally, risk appetites are a key influence, along with the cost/benefit of mitigation considerations, when determining the Target Risk Ratings of specific risks. Understanding and applying effective risk appetite considerations is highly beneficial in managing risk.

Inverell Shire Council has articulated its appetite for taking, retaining or accepting risk through qualitative Risk Appetite Statements that are based on nominated risk categories. Council has chosen to identify its risks within twelve risk categories that now contain primary and secondary positions of risk appetites.

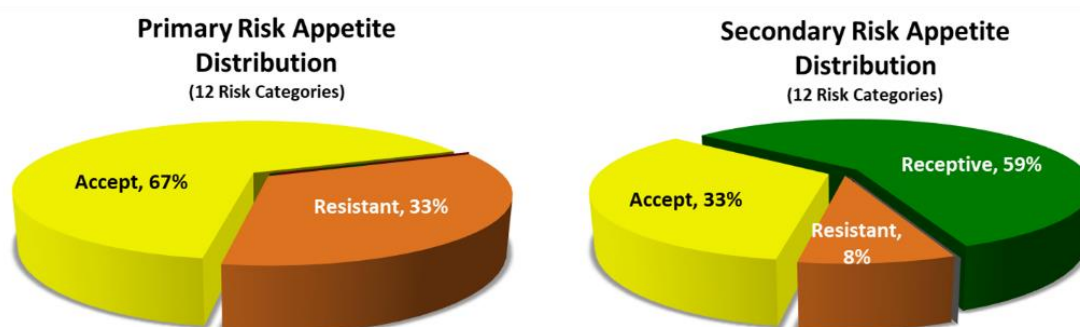
Through a workshop exercise involving Councillor's, Audit Risk and Improvement Committee members, and members of Council's Executive Leadership Team, risk appetite levels have been determined for each of Council's risk categories. The risk appetite levels produced are based on an ordinal scale of four levels: **Avoid**, **Resistant**, **Accept**, and **Receptive**. In this order, the levels provide an indication of an increasing willingness to take on, retain or accept risk, where Avoid and Resistant are considered more conservative, and Accept and Receptive are considered less conservative.

Inverell Shire Council has a primary risk appetite position that is considered less conservative. There are eight risk categories which have a primary risk appetite of **Accept** (67%) and four risk categories with a primary risk appetite of **Resistant** (33%). All of the risk categories have a secondary risk appetite distributed across three Risk Appetite levels. Of the secondary risk appetite positions, only one risk category (Financial) indicates a more conservative position to its primary position. The remainder move towards less conservative positions. The secondary risk appetite positions are: **Resistant** (1 category, or 8%) and **Accept** (4 categories, or 33%), and **Receptive** (7 categories, or 59%).

The distribution of primary and secondary risk appetite positions for Inverell Shire Council is indicative of a less conservative overall appetite towards taking, retaining or accepting risk. The distributions of primary and secondary levels of risk appetite for Council are illustrated in Diagram 1.

It should be noted that Risk Appetite Statements provide guidance only on Council's appetite for risk with regard to certain risk categories. There are many variable that should be considered in decision making, and the organisation's appetite for taking, retaining or accepting risk is only one of them.

Diagram 1 – Inverell Shire Council Primary and Secondary Risk Appetite Distributions



An important caveat to well-articulated qualitative Risk Appetite Statements is that they are, by their nature, not readily measurable (quantitative). In order to fully operationalise the concept of risk appetite, the development of several representative risk tolerance metrics for each risk category is required. These tolerances will provide an adjustable and ongoing ability to measure whether Council continues to operate within its stated risk appetites.



RISK APPETITE SUMMARY

The Risk Appetite Statements for Inverell Shire Council are based on the amount of risk that the Council is willing to take, retain or accept in pursuit of its objectives over the life of the current Operational Plan. The Council has a strategic focus on multiple areas, and many different and varied operations are carried out to support the Local Government Area. As such, appetites for risk can vary across these different operations and strategic focus areas. Therefore, Council's Risk Appetite Statements have been developed against each of Council's Risk Categories. These Statements use a four-level ordinal scale to indicate the amount of risk Council is willing to take, retain or accept for each category. Diagram 2 illustrates the four-level ordinal scale, with a definition for each.

Diagram 2: Risk Appetite Levels and Definitions

AVOID	RESISTANT	ACCEPT	RECEPTIVE
(little-to-no appetite)	(small appetite)	(medium appetite)	(larger appetite)
Avoidance of adverse exposure to risks even when outcome benefits are higher	A general preference for safer options with only small amounts of adverse exposure	Options selected based on outcome delivery with a reasonable degree of protection	Engagement with risks based more on outcome benefits than potential exposure

Table 1, provides a summary of Inverell Shire Council's risk appetite positions across its identified risk categories. Each category has one coloured cell, which represents the Primary Appetite position and one 'greyed' cell, which represents the Secondary Appetite position for those categories with an identified secondary appetite. These positions are defined as follows:

Primary Appetite: indicates a general appetite for taking, retaining or accepting risk for the given risk category.

Secondary Appetite: indicates an appetite-by-exception position for taking, retaining or accepting risk in specific circumstances. It is not necessary for all risk categories to have a Secondary Appetite position.

Table 1: Summary of Council's Risk Appetite positions

Category of Risk	Avoid	Resistant	Accept	Receptive
Financial		Secondary	Primary	
WH&S		Primary	Secondary	
People		Primary	Secondary	
Service Delivery			Primary	Secondary
Compliance		Primary	Secondary	
Environmental			Primary	Secondary
Reputation			Primary	Secondary
Information Technology			Primary	Secondary
Cyber Security		Primary	Secondary	
Property and Assets			Primary	Secondary
Project Budgets			Primary	Secondary
Project Timeframes			Primary	Secondary

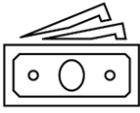



RISK APPETITE STATEMENTS


The tables below contain the primary and secondary Risk Appetite Statements for each risk category of Inverell Shire Council. These statements are qualitative in nature and designed to provide an indication of Council's general position when deciding to take, retain or accept risk, in pursuit of its strategic objectives.

Note: The effectiveness of Risk Appetite Statements will be improved through the development of quantifiable Risk Tolerances from representative metrics for each risk category.





▲ ▲ ▲ ▲ ▲ - Indicates the Secondary Risk Appetite

Financial		
	Level	Risk Appetite Statement
 Financial	Accept	<p>Regarding its Financial activities, Council is willing to Accept a medium level of risk in order to achieve its objectives. Council will endeavour to select options based on outcome delivery, whilst maintaining a reasonable degree of protection.</p> <p>▲ In certain circumstances, when considered appropriate, Council will adopt a more conservative Resistant position to Financial risks where safer options with smaller exposures are warranted.</p>





Work Health & Safety		
	Level	Risk Appetite Statement
 WH&S	Resistant	<p>In the pursuit of its objectives, Council seeks Resistant to adverse exposure to risks with regard to the Work Health & Safety of its employees, and any other people contracted to work for Council. Council's preferred position is for safer options with only small amounts of adverse exposure.</p> <p>▲ Council recognises that in certain circumstances it may need to Accept small amounts of exposure and is willing to do so in exceptional circumstances where there remains a reasonable degree of protection.</p>

People		
	Level	Risk Appetite Statement
 People	Resistant	<p>To achieve its objectives, Council has a small risk appetite and is Resistant to risk relating to its People. Notwithstanding the risk appetite levels of other risk categories where people are involved, with regard to its people Council has a general preference for safer options with only small amounts of adverse exposure.</p> <p>▲ Council recognises that in certain circumstances it may need to Accept small amounts of exposure and is willing to do so where there remains a reasonable degree of protection.</p>




Service Delivery		
		Risk Appetite Statement
 Service Delivery	Accept	<p>With regard to Service Delivery decisions and activities, Council is willing to Accept a medium level of risk in order to achieve its objectives. Council will endeavour to select options based on outcome delivery, whilst maintaining a reasonable degree of protection.</p> <p>▲ However, in some circumstances Council may be more Receptive to risk and focus more on outcome benefits.</p>
Compliance		
	Level	Risk Appetite Statement
 Compliance	Resistant	<p>In the pursuit of its objectives, Council is Resistant to risk in regard to Compliance with relevant legislation, regulations, standards, codes and/or policies. Council has only a small appetite for risk in these areas and prefers safer options with only small amounts of adverse exposure.</p> <p>▲ Council is, however, cognisant of the fact that in certain circumstances it will be prudent to Accept risk exposures so long as there remains a reasonable degree of protection.</p>
Environmental		
	Level	Risk Appetite Statement
 Environmental	Accept	<p>With regard to Environmental decisions and activities, Council is willing to Accept a medium level of risk in order to achieve its objectives. Council will endeavour to select options based on outcome delivery, whilst maintaining a reasonable degree of protection.</p> <p>▲ However, in some circumstances Council may be more Receptive to risk and focus more on outcome benefits.</p>
Reputation		
	Level	Risk Appetite Statement
 Reputation	Accept	<p>With regard to its Reputation, Council is willing to Accept a medium level of risk in order to achieve its objectives. Council will endeavour to select options based on outcome delivery, whilst maintaining a reasonable degree of protection.</p> <p>▲ However, in some circumstances Council may be more Receptive to risk and focus more on outcome benefits.</p>



Information Technology		
	Level	Risk Appetite Statement
	Accept	<p>With regard to its Information Technology, Council is willing to Accept a medium level of risk in order to achieve its objectives. Council will endeavour to select options based on outcome delivery, whilst maintaining a reasonable degree of protection.</p> <p>▲ However, in some circumstances Council may be more Receptive to risk and focus more on outcome benefits.</p>
Cyber Security		
	Level	Risk Appetite Statement
	Resistant	<p>In the pursuit of its objectives, Council is Resistant to risk in regard to Cyber Security. Council has only a small appetite for risk in this area and prefers safer options with only small amounts of adverse exposure.</p> <p>▲ Council is, however, cognisant of the fact that in certain circumstances it will be prudent to Accept risk exposures so long as there remains a reasonable degree of protection.</p>
Property & Assets		
	Level	Risk Appetite Statement
	Accept	<p>With regard to its Property & Assets, Council is willing to Accept a medium level of risk in order to achieve its objectives. Council will endeavour to select options based on outcome delivery, whilst maintaining a reasonable degree of protection.</p> <p>▲ However, in some circumstances Council may be more Receptive to risk and focus more on outcome benefits.</p>
Project Budgets		
	Level	Risk Appetite Statement
	Accept	<p>With regard to the setting and management of Project Budgets, Council is willing to Accept a medium level of risk in order to achieve its objectives. Council will endeavour to select options based on outcome delivery, whilst maintaining a reasonable degree of protection.</p> <p>▲ However, in some circumstances Council may be more Receptive to risk and focus more on outcome benefits.</p>



Project Timeframes		
	Level	Risk Appetite Statement
 Project Timeframes	Accept	<p>With regard to the setting and management of Project Timeframes, Council is willing to Accept a medium level of risk in order to achieve its objectives. Council will endeavour to select options based on outcome delivery, whilst maintaining a reasonable degree of protection.</p> <p>▲ However, in some circumstances Council may be more Receptive to risk and focus more on outcome benefits.</p>

CONCLUSION

The Risk Appetites expressed in this document will provide guidance to decision-makers as to where Council's general position is with regard to the level of risk it is willing to take, retain or accept in pursuit of its Strategies. The statements should be considered and reviewed during strategic planning and can be used as an influence when determining whether to increase or decrease control activity on specific risks, or whether to pursue opportunities. Additionally, it is better practice to review the Risk Appetite Statements thoroughly at least on a semi-annual basis and also every time there is a substantial shift in Inverell Shire Council's operating environment.

If more robust guidance is required, then Council should implement quantifiable risk tolerances for each of its risk categories. These tolerances will provide guidance on whether the risk appetite levels are set appropriately as well as provide indicative measures of whether Council is operating within its expressed appetite level for taking risks.

The development of Risk Appetite Statements is a very good start to Inverell Shire Council's risk management journey. This work will help the Council to continue an upward trajectory towards risk management maturity, and ultimately facilitate a capability for robust, repeatable and consistent quality decision-making.

CONTACTS

Name: Craig Hutley
 Title: Principal, Strategic Risk, Marsh Advisory, Pacific
 Practice Lead Queensland and Northern Territory
 Mobile: 0447 034 327
 Email: craig.hutley@marsh.com



STATEWIDE MUTUAL
PO Box H25
Australia Square NSW 1215
Tel: (02) 9320 2700
Fax: (02) 9320 2799
mail@statewide.nsw.gov.au
statewide.nsw.gov.au
ABN 69 009 098 864

5.2 GOVERNANCE - MONTHLY INVESTMENT REPORT**File Number:** S12.12.2 / 23/33086**Author:** Robert Kimmince, Manager Financial Services**SUMMARY:**

To report the balance of investments held as at 30 September, 2023.

RECOMMENDATION:

The Committee recommends to Council that:

- i) the report indicating Council's Fund Management position be received and noted; and*
- ii) the Certification of the Responsible Accounting Officer be noted.*

COMMENTARY:

Contained within this report are the following items that highlight Council's Investment Portfolio performance for the month to 30 September, 2023 and an update of the investment environment:

- (a) Council's Investments as at 30 September, 2023;
- (b) Council Investments by Fund as at 30 September, 2023;
- (c) Interest – Budgeted vs. Actual;
- (d) Investment Portfolio Performance;
- (e) Investment Commentary; and
- (f) Certification – Responsible Accounting Officer.

A) Council Investments as at 30 September, 2023

Term Deposit Investment Group										
Investment	Borrower	FUND	Rating	Interest Frequency	Purchase Date	Maturity Date	Current Yield	Principal Value	Current value	Term (days)
23/44	Hume Bank	General		Maturity	28-Jun-23	01-Oct-23	5.30%	1,000,000	1,000,000	95
23/27	Bank of Queensland	General	BBB+	Maturity	29-Mar-23	01-Oct-23	4.60%	2,000,000	2,000,000	186
23/12	Suncorp	Sewer	A	Maturity	05-Oct-22	05-Oct-23	4.33%	1,500,000	1,500,000	365
23/10	AMP BANK	General	BBB+	Maturity	05-Oct-22	05-Oct-23	4.30%	2,000,000	2,000,000	365
22/09	National Australia Bank	General	AA-	Annually	06-Oct-21	06-Oct-23	0.64%	1,000,000	1,000,000	730
23/13	Westpac Bank	General	AA-	Quarterly	19-Oct-22	19-Oct-23	4.43%	2,000,000	2,000,000	365
22/10	Westpac Bank	General	AA-	Quarterly	25-Oct-21	25-Oct-23	0.91%	2,000,000	2,000,000	730
22/11	Westpac Bank	General	AA-	Quarterly	25-Nov-21	27-Nov-23	1.28%	1,000,000	1,000,000	732
22/28	AMP BANK	General	BBB+	Maturity	27-May-22	27-Nov-23	3.30%	2,000,000	2,000,000	549
23/17	AMP Bank	Water	BBB	Annually	25-Nov-22	27-Nov-23	4.60%	1,000,000	1,000,000	367
22/27	Australian Unity Bank	General	BBB	Annually	26-May-22	27-Nov-23	3.50%	1,000,000	1,000,000	550
23/33	Bank of Queensland	General		Maturity	29-May-23	29-Nov-23	5.01%	1,500,000	1,500,000	184
22/15	ICBC - Industrial and Commercial Bank of China	General	A	Annually	02-Dec-21	04-Dec-23	1.36%	2,000,000	2,000,000	732
22/16	ICBC - Industrial and Commercial Bank of China	General	A	Annually	02-Dec-21	04-Dec-23	1.36%	2,000,000	2,000,000	732
22/17	ICBC - Industrial and Commercial Bank of China	Water	A	Annually	02-Dec-21	04-Dec-23	1.36%	1,000,000	1,000,000	732
23/18	Bank of Sydney	General	NR	Annually	07-Dec-22	07-Dec-23	4.60%	2,000,000	2,000,000	365
23/42	Hume Bank	General		Maturity	28-Jun-23	28-Dec-23	5.65%	2,000,000	2,000,000	183
23/35	Australian Military Bank	General		Maturity	29-May-23	29-Dec-23	5.05%	2,000,000	2,000,000	214
23/20	ING Bank	General	A	Annually	23-Jan-23	23-Jan-24	4.50%	1,500,000	1,500,000	365
23/25	Bank of Sydney	General	Unrated	Quarterly	24-Mar-23	24-Jan-24	4.70%	2,000,000	2,000,000	306
23/28	BoQ	General	BBB	Annually	19-Apr-23	19-Jan-24	4.70%	2,000,000	2,000,000	275
23/21	Commonwealth Bank	Sewer	AA	Annually	27-Feb-23	27-Feb-24	5.06%	2,000,000	2,000,000	365
23/36	Bendigo & Adelaide	General	BBB	Maturity	31-May-23	29-Feb-24	5.00%	1,500,000	1,500,000	274
22/20	MyState Bank	General	BBB	Maturity	02-Mar-22	04-Mar-24	1.70%	2,000,000	2,000,000	733
22/21	Bank of Queensland	General	BBB+	Quarterly	02-Mar-22	04-Mar-24	1.70%	1,000,000	1,000,000	733
23/22	AMP BANK	General	BBB+	Annually	20-Mar-23	20-Mar-24	4.80%	1,000,000	1,000,000	366
23/23	Bank of Sydney	Water	BBB+	Maturity	20-Mar-23	20-Mar-24	4.85%	1,500,000	1,500,000	366
21/11	ICBC - Industrial and Commercial Bank of China	Water	A	Annually	26-Mar-21	26-Mar-24	0.82%	2,000,000	2,000,000	1096
23/43	MyState Bank	General		Maturity	28-Jun-23	28-Mar-24	5.60%	2,000,000	2,000,000	274
23/30	Police Credit Union	General	Unrated	Maturity	08-May-23	08-May-24	4.85%	1,000,000	1,000,000	366
23/37	Suncorp	General	A+	Maturity	31-May-23	30-Apr-24	4.96%	2,000,000	2,000,000	335
23/29	Police Credit Union	Water	Unrated	Maturity	08-May-23	08-May-24	4.85%	1,000,000	1,000,000	366
23/31	AMP BANK	General	BBB+	Annually	25-May-23	27-May-24	5.15%	1,000,000	1,000,000	368
23/38	ING Bank	General	A	Maturity	31-May-23	30-May-24	5.10%	1,500,000	1,500,000	365
23/32	AMP BANK	General	BBB+	Annually	25-May-23	27-May-24	5.15%	1,000,000	1,000,000	368
23/39	Suncorp	Sewer	A	Maturity	07-Jun-23	07-Jun-24	5.26%	1,000,000	1,000,000	366
23/40	Australian Unity Bank	General	BBB+	Annually	20-Jun-23	20-Jun-24	5.60%	1,500,000	1,500,000	366
23/45	National Australia Bank	Water	AA-	Annually	29-Jun-23	28-Jun-24	5.45%	2,000,000	2,000,000	365
23/41	National Australia Bank	Water	AA-	Annually	28-Jun-23	28-Jun-24	5.55%	1,000,000	1,000,000	366
24/02	Bank of Sydney	General	Unrated	Annually	27-Jul-23	29-Jul-24	5.45%	2,000,000	2,000,000	368
24/01	AMP BANK	General	BBB	Annually	27-Jul-23	29-Jul-24	5.55%	2,000,000	2,000,000	368
24/04	Police Credit Union	General	Unrated	Maturity	08-Aug-23	08-Aug-24	5.35%	1,000,000	1,000,000	366
22/03	National Australia Bank	General	AA-	Annually	27-Aug-21	27-Aug-24	0.85%	2,000,000	2,000,000	1096
24/05	National Australia Bank	General	AA-	Maturity	29-Aug-23	29-Aug-24	5.24%	1,500,000	1,500,000	366
24/03	Police Credit Union	General	Unrated	Maturity	04-Aug-23	06-Aug-24	5.35%	1,000,000	1,000,000	368
24/06	National Bank Australia	General	BBB+	Maturity	07-Sep-23	09-Sep-24	5.23%	2,000,000	2,000,000	368
24/07	National Australia Bank	General	AA	Annually	13-Sep-23	13-Sep-24	5.24%	1,000,000	1,000,000	366
24/08	National Australia Bank	General	AA-	Maturity	13-Sep-23	13-Sep-24	5.24%	2,000,000	2,000,000	366
24/09	National Australia Bank	General	AA-	Maturity	13-Sep-23	13-Sep-24	5.24%	2,000,000	2,000,000	366
24/10	NAB	Water	AA-	Annually	20-Sep-23	20-Sep-24	5.30%	1,000,000	1,000,000	366
24/11	NAB	Sewer	AA-	Annually	20-Sep-23	20-Sep-24	5.30%	1,000,000	1,000,000	366
23/11	ING Bank	General	A	Quarterly	05-Oct-22	08-Oct-24	4.75%	2,000,000	2,000,000	734
23/26	Auswide Bank	General	BBB	Monthly	24-Mar-23	24-Mar-25	4.80%	1,000,000	1,000,000	731
23/24	Auswide Bank	Water	BBB	Monthly	24-Mar-23	24-Mar-25	4.80%	1,000,000	1,000,000	731
21/13	ICBC - Industrial and Commercial Bank of China	Water	A	Annually	27-May-21	27-May-26	1.40%	1,000,000	1,000,000	1826
21/14	ICBC - Industrial and Commercial Bank of China	Sewer	A	Annually	27-May-21	27-May-26	1.40%	1,000,000	1,000,000	1826
21/15	ICBC - Industrial and Commercial Bank of China	General	A	Annually	27-May-21	27-May-26	1.40%	1,000,000	1,000,000	1826
TOTALS								86,000,000	86,000,000	

Cash Deposit Accounts										
As at Date	Borrower	FUND	Rating		Purchase Date	Maturity Date	Current Yield	Value at beg year	Current value	Term
30/9/23	Commonwealth Bank	General	A		9/11/2020		0.00%		1,194.89	
30/9/23	Macquarie Bank	General	AA-	Monthly	9/11/2020		3.90%	2,086,371	2,100,443.86	
30/9/23	Macquarie Bank	Water	AA-	Monthly	9/11/2020		3.90%	2,588,269	2,605,727.03	
30/9/23	Macquarie Bank	Sewer	AA-	Monthly	9/11/2020		3.90%	1,551,712	1,562,178.52	
Sub Total - Cash Deposit Accounts									6,269,544.30	-

B) Council Investments by Fund 30 September, 2023

Portfolio by Fund	31/08/2023	30/09/2023
General Fund	\$69,101,639	\$69,101,639
Water Fund	\$15,105,727	\$15,105,727
Sewer Fund	\$8,062,179	\$8,062,179
TOTAL	\$92,269,544	\$92,269,544

Council's investment portfolio remained neutral throughout September 2023. This was in respect of normal cash flow movements for receipts collected and payments made during September 2023.

Interest – Budgeted verses Actual Result to Date

	Ledger	2023/2024 Budget \$	Actuals to Date \$	Accrued Interest to Date \$	TOTAL \$
General Fund	128820	884,000	313,047	217,156	530,203
Water Fund	812350	182,000	21,589	45,305	66,894
Sewer Fund	906320	130,000	9,587	27,723	37,310
TOTAL		1,196,000	344,223	290,184	634,407

Term deposit interest rates have improved recently with a 12-month term deposit now yielding 4-80 – 5.20%. Given our strong investment balances, Council is expected to exceed interest revenue targets in 2023/2024. This additional interest received during 2023/2024 will be allocated to special projects during 2024/2025.

C) Investment Portfolio Performance

Investment Portfolio Return		Benchmarks		
	% pa	RBA Cash Rate	Aus Bond Bank Bill	11am Cash Rate
Benchmark as at 30/9/2023		4.10%	4.11%	4.10%
Term Deposits	4.12%			
Cash Deposit Accounts	3.90%			
180 Day Call Account	0.00%			
Floating Rate Notes	0.00%			

D) Investment Commentary

Council's investment portfolio returns exceeded the above benchmarks in all investment categories except for Council's cash deposit accounts. These accounts are held for liquidity purposes.

Council's investment portfolio of \$92.2M is almost entirely invested in fixed term deposits. Overall, the portfolio is highly liquid, highly rated and short-dated from a counterparty perspective.

Certification – Responsible Accounting Officer

I Paul Pay, hereby certify that the investments listed in this report have been made in accordance with Section 625 of the *Local Government Act 1993*, Clause 212 of the Local Government (General) Regulations 2005 and Council's Investment Policy.

RISK ASSESSMENT:

Nil

POLICY IMPLICATIONS:

Nil

CHIEF FINANCIAL OFFICERS COMMENT:

Council's term deposit portfolio was yielding 4.12% p.a. at month-end, with a weighted average duration of around 200 days or 6.6 months. Council is well positioned to take advantage of increasing term deposit rates as investments mature.

LEGAL IMPLICATIONS:

Nil

ATTACHMENTS:

Nil

6 CONFIDENTIAL MATTERS (COMMITTEE-OF-THE-WHOLE)**RECOMMENDATION:**

That Council considers the confidential report(s) listed below in a meeting closed to the public in accordance with the reasons stated in the referral reports:

6.1 Outstanding Debtor Account - 215057-1