AGENDA

FINANCE AND GOVERNANCE COMMITTEE

Tuesday, 14 October 2025
10 minutes after the conclusion of the Infrastructure, Planning and Assets Committee or such later time as determined by the preceding committee

Council Chambers, Level 8
1 Nicholas Street, Ipswich

MEMBERS OF THE FINANCE AND GOVERNANCE COMMITTEE	
Councillor Paul Tully **(Chairperson)** Councillor Jacob Madsen **(Deputy Chairperson)**	Mayor Teresa Harding Deputy Mayor Nicole Jonic Councillor Marnie Doyle Councillor Andrew Antoniolli Councillor Jim Madden

FINANCE AND GOVERNANCE COMMITTEE AGENDA

** Item includes confidential papers

FINANCE AND GOVERNANCE COMMITTEE NO. 2025(09)

14 OCTOBER 2025

AGENDA

WELCOME TO COUNTRY OR ACKNOWLEDGEMENT OF COUNTRY

DECLARATIONS OF INTEREST IN MATTERS ON THE AGENDA

BUSINESS OUTSTANDING

CONFIRMATION OF MINUTES

1. CONFIRMATION OF MINUTES OF THE FINANCE AND GOVERNANCE COMMITTEE NO. 2025(08) OF 16 SEPTEMBER 2025

RECOMMENDATION

That the minutes of the Finance and Governance Committee held on 16 September 2025 be confirmed.

OFFICERS' REPORTS

2. LEASE RENEWAL OF FREEHOLD LAND AT 116 BRISBANE STREET, IPSWICH

This is a report concerning the proposed lease renewal over freehold land located at 116 Brisbane Street, Ipswich, described as part of Lot 12 on SP103223 (the Land), between Ipswich City Council (Council) and Rajesh Sharma.

RECOMMENDATION

A. That pursuant to section 236(2) of the *Local Government Regulation 2012* (Regulation), Council resolve that the exception at section 236(1)(c)(iii) of the Regulation applies to the disposal of interest in land at 116 Brisbane Street, Ipswich more particularly described as part of Lot 12 and Plan SP103223, for restaurant purposes, because it is for renewal of a lease to the existing lessee.

B. That Council renew the lease (Council file reference number 6430 with Rajesh Sharma (Lessee):

(i) at a commencing annual rent of $85,603.09 plus CPI excluding GST, payable to Council, and
(ii) for a term of five (5) years, with no options for extension.

---

3. INFORMATION AND CYBER SECURITY POLICY

This is a report concerning the review and update of the Information and Cyber Security Policy.

RECOMMENDATION

That the Finance and Governance Committee approve the updated Information and Cyber Security Policy in accordance with the standard four-year development and improvement cycle as detailed in Attachment 3.

NOTICES OF MOTION

MATTERS ARISING

QUESTIONS / GENERAL BUSINESS

FINANCE AND GOVERNANCE COMMITTEE NO. 2025(08)

16 SEPTEMBER 2025

MINUTES

COUNCILLORS' ATTENDANCE:

Councillor Paul Tully (Chairperson); Councillors Nicole Jonic, Andrew Antoniolli, Jim Madden and Pye Augustine (Observer) and David Martin (Observer)

COUNCILLOR'S APOLOGIES:

Mayor Teresa Harding

OFFICERS' ATTENDANCE:

Chief Executive Officer (Sonia Cooper), General Manager Corporate Services (Matt Smith), General Manager Community, Cultural and Economic Development (Ben Pole), Acting General Manager Environment and Sustainability (Phil A Smith), General Manager Planning and Regulatory Services (Brett Davey), General Manager Asset and Infrastructure Services (Seren McKenzie), Manager, City Design (Nathan Rule), Property Services Manager (Alicia Rieck), Chief Financial Officer (Christina Binoya), Manager, Works and Field Services (Sonia Gollschewski), Senior Media Officer (Darrell Giles), Manager, Media, Communications and Engagement (Mark D Strong), Senior Communications and Policy Officer (Jodie Richter), Chief of Staff – Office of the Mayor (Melissa Fitzgerald), Manager, Procurement (Tanya Houwen), Goods and Services Category Manager (Tim Steinhardt) and Venue Technician (Max Moylan)

WELCOME TO COUNTRY OR ACKNOWLEDGEMENT OF COUNTRY

Councillor Paul Tully (Chairperson) delivered the Acknowledgement of Country

DECLARATIONS OF INTEREST IN MATTERS ON THE AGENDA

Nil

BUSINESS OUTSTANDING

1. PROPOSED DISPOSAL OF VALUABLE NON-CURRENT LAND ASSETS

*At the Finance and Governance Committee held on 19 August 2025, this matter was deferred for consideration at the September Finance and Governance Committee Meeting***.**

This is a report concerning a recent review of Council's *'Program 43'* (Corporate Services Department) land portfolio which has identified land considered surplus

to Council's requirements and seeks approval from Council to proceed with the disposal of these assets.

"The attachment/s to this report are confidential in accordance with section 254J(3)(g) of the *Local Government Regulation 2012*."

RECOMMENDATION

Moved by Acting Mayor Nicole Jonic:
Seconded by Councillor Andrew Antoniolli:

A. That pursuant to Section 228 of the *Local Government Regulation 2012* (Regulation), Council award Tenders for the disposal of land as described in Attachment 1, to the Purchaser(s).

B. That pursuant to section 236(2) of the *Local Government Regulation 2012* (Regulation), Council resolve that an exception at section 236(1) of the Regulation applies to the disposal of land as described in Attachment 1.

C. That for each sale, Council enter into a contractual arrangement with the Purchaser(s) at an approximate sale price no less than the market value of the land (excluding GST), payable to Council.

D. That pursuant to Section 257(1)(b) of the *Local Government Act 2009*, Council resolve to delegate to the Chief Executive Officer the power to take "*contractual action"* pursuant to section 238 of the Regulation, in order to implement Council's decision.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

CONFIRMATION OF MINUTES

2. CONFIRMATION OF MINUTES OF THE FINANCE AND GOVERNANCE COMMITTEE NO. 2025(07) OF 19 AUGUST 2025

RECOMMENDATION

Moved by Councillor Jim Madden:
Seconded by Councillor Marnie Doyle:

That the minutes of the Finance and Governance Committee held on 19 August 2025 be confirmed.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

OFFICERS' REPORTS

3. AMENDMENT OF COUNCIL RESOLUTIONS FOR PROPOSED ACQUISITIONS OF LAND FOR RIPLEY AND FISCHER ROAD UPGRADES

This is a report concerning two (2) previous Council decisions and the proposed amendment to the Confidential Attachment 1 of each report, both detailing the area(s) of land required for Stage 2 and 3 of the Ripley and Fischer Road Upgrade Project, by acquisition.

"The attachment/s to this report are confidential in accordance with section 254J(3)(h) of the *Local Government Regulation 2012*."

RECOMMENDATION

Moved by Councillor Marnie Doyle:
Seconded by Acting Mayor Nicole Jonic:

A. That the decision of Council of 24 October 2024 (Resolution Number: C2024/08/290(FAGCC) relating to Recommendation A of Item 7 of the Finance and Governance Committee of 15 October 2024 titled *Proposed Acquisitions of Land for INF04658 Ripley Road Upgrade – Cunningham Highway to Fischer Road*, be amended by replacing the original Confidential Attachment 1 with an updated Confidential Attachment 5 outlining the revised area requirement for the land acquisitions.

B. That the decision of Council of 28 January 2025 (Resolution Number: C2025/00/273 relating to Recommendation A of Item 16.4 of the Council meeting of 28 January 2025 titled *Proposed Acquisition of Land for INF04659 Fischer Road Upgrade*, be amended by replacing the original Confidential Attachment 1 with an updated Confidential Attachment 5 outlining the revised area requirement for the land acquisition.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

---

4. FUTURE OF OLD TALLEGALLA SCHOOL, 2 TALLEGALLA TWO TREE HILL ROAD, TALLEGALLA

This is a report concerning the current Action Notice relating to the Old Tallegalla School, located at 2 Tallegalla Two Tree Hill Road, Tallegalla. It seeks Council's direction on the next steps regarding the future of the site, including further consideration of the outcome of the community consultation.

RECOMMENDATION

Moved by Councillor Jim Madden:
Seconded by Councillor Andrew Antoniolli:

That pursuant to Section 228(3)(a) of the *Local Government Regulation 2012* (Regulation), Council resolve that it would be in the public interest to invite expressions of interest for disposal of leasehold interest in land (trustee lease) at 2 Tallegalla Two Tree Hill Road, Tallegalla more particularly described as Lot 557 and Plan CC3651 for community purpose.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

---

5. CONFLICT OF INTEREST FOR EMPLOYEES POLICY REVIEW

This report details the outcome of the required four year review of the existing Conflicts of Interest for Employees Policy. It was considered by the Executive Leadership Team on 15 July and has been referred to the Finance and Governance Committee for approval.

RECOMMENDATION

Moved by Councillor Andrew Antoniolli:
Seconded by Acting Mayor Nicole Jonic:

That the amended Conflicts of Interest for Employees Policy as outlined in Attachment 3, be adopted.

AFFIRMATIVE	NEGATIVE
Councillors:	Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

6. PROCUREMENT - VARIATION TO CONTRACT FOR PROVISION OF COMMERCIAL CLEANING

This is a report concerning a request for Council's approval to extend Contract No. 13902 for commercial cleaning services by six months beyond its current expiry date of 1 December 2025. The extension is necessary to maintain service continuity during the school holidays and festive period while the procurement process for a new contract is being finalised.

Approval is sought to vary the existing contract 13902 for an additional six (6) months to allow additional time to thoroughly evaluate tender submissions received as part of the new procurement process and allow a suitable transition time (if required) outside of peak holiday periods.

RECOMMENDATION

Moved by Councillor Jim Madden:

Seconded by Councillor Jacob Madsen:

A. That the contractual arrangement (Council contract 13902) with Total Building Maintenance (Supplier) for the Provision of Commercial Cleaning be varied as follows:

(i) Add a final extension of six (6) months (from 1 December 2025 to 31 May 2026);

(ii) to approve increase in expenditure from $10,500,000.00 excluding GST to approximately $12,500,000.00 excluding GST over the entire term;

B. That Council enter into a deed of variation with the Supplier to appropriately amend the existing contractual arrangement.

C. That pursuant to Section 257(1)(b) of the *Local Government Act 2009*, Council resolve to delegate to the Chief Executive Officer the power to take "*contractual action"* pursuant to section 238 of the Regulation, in order to implement Council's decision.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

ADJOURN MEETING

RECOMMENDATION

Moved by Councillor Paul Tully:
Seconded by Acting Mayor Nicole Jonic:

That the meeting be adjourned at 10.04 am to reconvene at 10.20 am.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	

Antoniolli
Madden

The motion was put and carried.

The meeting reconvened at 10.20 am.

At recommencement of the meeting all councillors with the exception of Councillors Jacob Madsen and Marnie Doyle were present.

---

7. PROCUREMENT: SIGNIFICANT CONTRACTING PLAN - TIVOLI SPORTING COMPLEX UPGRADE AND REDBANK PLAINS RECREATION RESERVE NEW SPORTS FACILITY

This is a report concerning a Significant Contracting Plan for Tivoli Sporting Complex Upgrade and Redbank Plains Recreation Reserve New Sports Facility.

The Significant Contracting Plan is required in accordance with Chapter 6, Part 2, s221 of the Local Government Regulation 2012 for any contract/s with a total expected term over 10 years or a value equal to or exceeding $7,000,000 (ex. GST). Significant Contracting Plans must be adopted by Council prior to awarding a contract.

RECOMMENDATION

Moved by Councillor Paul Tully:
Seconded by Councillor Jim Madden:

That pursuant to Section 221 of the *Local Government Regulation 2012*, Council make and adopt the Significant Contracting Plan for Tivoli Sporting Complex Upgrade and Redbank Plains Recreation Reserve New Sports Facility as detailed in Attachment 1.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Jonic	
Antoniolli	
Madden	

The motion was put and carried.

---

8. PROCUREMENT: INTERSECTION UPGRADE – RIPLEY ROAD & REIF STREET, FLINDERS VIEW

This is a report concerning the approval for the award of Tender VP465457 Intersection Upgrade, Ripley Road and Reif Street, Flinders View.

After an open market request for tender process, the evaluation panel has recommended one supplier for the undertaking of the intersection upgrade, Ripley Road and Reif Street as set out in Recommendation B below. The recommendation has been determined by the evaluation panel to offer Council the best value for money

If Council is satisfied with the nominated supplier, the name of the supplier will be included in Council's resolution at Recommendation B.

"The attachment/s to this report are confidential in accordance with section 254J(3)(g) of the *Local Government Regulation 2012*."

Councillor Marnie Doyle returned to the meeting at 10.24 am.

RECOMMENDATION

Moved by Acting Mayor Nicole Jonic:
Seconded by Councillor Jim Madden:

A. That pursuant to Section 228 of the *Local Government Regulation 2012* (Regulation), Council award Tender No. VP465457 for the provision of Intersection Upgrade – Ripley Road and Reif Street, Flinders View.

B. That Council enter into a contractual arrangement with the Supplier identified in the confidential Attachment 1 for the lump sum amount of two million, seven hundred sixty-eight thousand, one hundred sixty-eight dollars ($2,768,168.00) excluding GST and the contingency amount as listed in confidential Attachment 1.

C. That pursuant to Section 257(1)(b) of the *Local Government Act 2009*, Council resolve to delegate to the Chief Executive Officer the power to take "*contractual action*" pursuant to section 238 of the Regulation, in order to implement Council's decision.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

Councillor Jacob Madsen returned to the meeting at 10.26 am.

9. PROCUREMENT: RECOMMENDATION TO AWARD - INTELLIGENT TRAFFIC SYSTEM INFRASTRUCTURE (TRAFFIC SIGNAL MAINTENANCE)

This is a report concerning the recommendation to award for Tender VP430214 Intelligent Transport System Infrastructure (Traffic Signal Maintenance) following an Open Tender process.

"The attachment/s to this report are confidential in accordance with section 254J(3)(g) of the *Local Government Regulation 2012*."

RECOMMENDATION

Moved by Councillor Jacob Madsen:
Seconded by Councillor Andrew Antoniolli:

A. That pursuant to Section 228 of the Local Government Regulation 2012 (Regulation), Council award Tender VP430214 for the provision of Intelligent Transport System Infrastructure to the recommended supplier detailed in Attachment 1.

B. That Council enter into a contractual arrangement with the Supplier, Council's estimated spend of $10.5M excluding GST, being a term of two (2) years, with options for extension at the discretion of Council (as purchaser), of an additional two (2) X two (2) year terms, total term being six (6) years.

C. That pursuant to Section 257(1)(b) of the *Local Government Act 2009*, Council resolve to delegate to the Chief Executive Officer the power to take "*contractual action*" pursuant to section 238 of the Regulation, in order to implement Council's decision.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

---

10. REPORT - REGULATION ADVISORY COMMITTEE NO. 2025(03) OF 21 AUGUST 2025

This is the report of the Regulation Advisory Committee No. 2025(03) of 21 August 2025.

RECOMMENDATION

Moved by Councillor Marnie Doyle:
Seconded by Councillor Jim Madden:

That Council adopt the recommendations of the Regulation Advisory Committee No. 2025(03) of 21 August 2025.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

---

1. CONFIRMATION OF MINUTES OF THE REGULATION ADVISORY COMMITTEE NO. 2025(02) OF 5 JUNE 2025

RECOMMENDATION

That the minutes of the Regulation Advisory Committee held on 5 June 2025 be confirmed.

2. STRATEGIC REGULATION PROJECT - STEP 1 POLICY (CONSULTATION OUTCOMES)

This is a report concerning the Strategic Regulation Project, specifically Step 1 which involves updating Council's current Compliance and Enforcement Policy to be more holistic on what Council's position on regulation is. Targeted consultation has been undertaken, and this report provides the outcomes of that consultation and next steps.

RECOMMENDATION

A. That the report be received and the contents noted.

B. That the current Compliance and Enforcement Policy (Attachment 1) be amended to be more holistic about regulation with a risk-based approach and renamed to 'Regulation Policy'.

C. That in respect of Recommendation B, the draft 'Regulation Policy' be forwarded to all Councillors and key staff for feedback, and a final draft be forwarded to a future Regulation Advisory Committee meeting for consideration.

The committee discussed the naming of the proposed amended policy and compressed Recommendations B and C noting that feedback would be sought and an updated policy forwarded to a future Regulation Advisory Committee.

RECOMMENDATION

A. That the report be received and the contents noted.

B. That the current Compliance and Enforcement Policy (Attachment 1) be amended and the draft be forwarded to all Councillors and key staff for feedback, and a final draft be forwarded to a future Regulation Advisory Committee meeting for consideration.

3. STRATEGIC REGULATION PROJECT - STEP 2 - LOCAL LAW MAKING PROCESS

This is a report concerning Step 2 of the Strategic Regulation Project the process for making local laws in line with the requirements of the Local Government Act 2009. The report highlights that the current policy can be repealed as it is not legislatively required and is set out like a process. An improved draft process is provided for feedback so that it can be finalised and commence on 1 December 2025.

The committee agreed to amend Recommendation B by replacing the word 'Council' with the words 'Councillors and officers'.

RECOMMENDATION

A. That Council repeal the "Local Law-Making Policy" effective as of 30 November 2025 (Attachment 1 of this report).

B. That Councillors and officers provide feedback on the draft process (Attachment 2 of this report) by 1 November 2025 so that the draft process can be finalised and approved by the Chief Executive Officer for commencement on 1 December 2025.

4. *STRATEGIC REGULATION PROJECT - STEP 3 LOCAL LAW REVIEW ESTIMATED TIMEFRAMES*

This is a report concerning a request from the Regulation Advisory Committee to review the timeline of the local law review with a view to compressing the estimated completion time. Negotiable and not negotiable tasks have been identified with three options provided for discussion, along with the recommendation of Council officers preferred option, Option 2, which comprises of:

- *Reduction of 2 weeks for community consultation in phase 3 (from 6 weeks down to 4 weeks)*
- *Reduction of Phase 5 (Drafting) from 6 months down to 5 months.*
- *Total reduction of one month and 2 weeks*
- *Estimated completion date of March 2027.*
  - *This would result in the final report for consideration of the final laws occurring early March at a Regulation Advisory Committee meeting and subsequent Finance and Governance Committee and Ordinary Council meetings.*
  - *Acknowledgement of the risks identified in this report for reducing drafting time.*

RECOMMENDATION

A. That the report be received and the contents noted.

B. That Option 2 of the report be approved as the preferred option for compressing the estimated completion time for the Local Law Review.

5. *STRATEGIC REGULATION PROJECT - STEP 3 LOCAL LAW REVIEW SURVEY OUTCOMES (INTERNAL)*

This is a report providing an update on a recent internal survey of staff and Councillors for the Strategic Regulation Project: Step 3 Local Law Review. The report documents the high-level key themes that have been derived from the submissions received. Further meetings/workshops will be held to progress outcomes of the survey.

RECOMMENDATION

That the report be received and the contents noted.

7. *GENERAL DISCUSSION (within the purpose and scope of the committee)*

The committee discussed regulatory matters relating to:

- Homelessness and rough sleepers
- Unregistered cars
- Squatters
- Unmade Road Reserves

Councillor Paul Tully (Chairperson) raised the issue of access to unmade road reserves and to the Notice of Motion he moved at the 30 April 2025 Council meeting in relation to unlocking of barriers across road reserves.

Action: Chief Executive Officer to follow up on action.

---

11. MONTHLY FINANCIAL PERFORMANCE REPORT - AUGUST 2025

This is a report concerning Ipswich City Council's (**Council**) financial performance for the period ending 31 August 2025, submitted in accordance with section 204 of the *Local Government Regulation 2012*.

RECOMMENDATION

Moved by Acting Mayor Nicole Jonic:
Seconded by Councillor Marnie Doyle:

That the report on Council's financial performance for the period ending 31 August 2025, submitted in accordance with section 204 of the *Local Government Regulation 2012*, be considered and noted by Council.

AFFIRMATIVE Councillors:	NEGATIVE Councillors:
Tully	Nil
Madsen	
Jonic	
Doyle	
Antoniolli	
Madden	

The motion was put and carried.

NOTICES OF MOTION

Nil

MATTERS ARISING

Nil

QUESTIONS / GENERAL BUSINESS

Nil

PROCEDURAL MOTIONS AND FORMAL MATTERS

The meeting commenced at 9.52 am.

The meeting closed at 10.33 am.

Doc ID No: A12023375

ITEM: 2

SUBJECT: LEASE RENEWAL OF FREEHOLD LAND AT 116 BRISBANE STREET, IPSWICH

AUTHOR: SENIOR PROPERTY OFFICER (TENURE)

DATE: 24 SEPTEMBER 2025

EXECUTIVE SUMMARY

This is a report concerning the proposed lease renewal over freehold land located at 116 Brisbane Street, Ipswich, described as part of Lot 12 on SP103223 (the Land), between Ipswich City Council (Council) and Rajesh Sharma.

RECOMMENDATION

A. That pursuant to section 236(2) of the *Local Government Regulation 2012* (Regulation), Council resolve that the exception at section 236(1)(c)(iii) of the Regulation applies to the disposal of interest in land at 116 Brisbane Street, Ipswich more particularly described as part of Lot 12 and Plan SP103223, for restaurant purposes, because it is for renewal of a lease to the existing lessee.

B. That Council renew the lease (Council file reference number 6430 with Rajesh Sharma (Lessee):

(i) at a commencing annual rent of $85,603.09 plus CPI excluding GST, payable to Council, and
(ii) for a term of five (5) years, with no options for extension.

RELATED PARTIES

- Rajesh Sharma
- There was no declaration of conflicts of interest

IFUTURE THEME

A Trusted and Leading Organisation

PURPOSE OF REPORT/BACKGROUND

The premises at 116 Brisbane Street, Ipswich are currently leased to Rajesh Sharma, trading as Indian Mehfil Restaurant, under a Council lease expiring 30 June 2026.

The building is State heritage listed, originally constructed in 1878 as the Bank of Australasia with an attached manager's residence. Following its closure in 1943, the property remained vacant until acquired by Ipswich City Council in 1985. Since acquisition, it has

served various civic functions including use as Council offices, the Ipswich Library, and the Visitor Information Centre.

In 2003, Council tendered the premises for restaurant use, awarding the contract to D'Arcy's on Doyle Restaurant and Bar in 2004. A lease was entered into in October 2006 but terminated in December 2007.

In 2008, Council entered into a lease with Adana Corporation Pty Ltd for a Turkish restaurant. In May 2010, the lease was assigned to Rajesh Sharma, who has operated the Indian Mehfil Restaurant since.

The current lease includes three additional licence areas for outdoor dining, café, and storage. Mr Sharma has agreed to amend the café and rear outdoor dining area previously known as 116 Laneway café & bar which has remained inactive since the COVID-19 pandemic.

FUTURE USE OF THE PROPERTY

The Council-owned property at 116 Brisbane Street occupies a prominent location in the Ipswich CBD, adjacent to d'Arcy Doyle Place and surrounded by heritage buildings. Its strategic position presents an opportunity to enhance the city's Arts Precinct, particularly in support of the Ipswich Art Gallery.

The building's heritage character and proximity to the Art Gallery make it well-suited for integration into the precinct, offering both cultural value and commercial potential. However, its current lease arrangement may limit longer term activation opportunities.

Council has secured grant funding to commence planning for the Arts Precinct. While the immediate focus remains on activating the Nicholas Street Precinct, officers propose to begin exploring future use options for 116 Brisbane Street.

The proposed lease terms are as follows;

Lease Terms	Existing	Proposed
Period:	5 Years	5 Years
Commencement Date:	01/07/2021	01/07/2026
Expiry Date:	30/06/2026	30/06/2031
Commencing Rent:	$77,892.24 (excluding GST)	$85,603.09 (excluding GST) plus CPI
Existing Rent:	$85,603.09 (excluding GST)	-
Annual Increase:	CPI	CPI
Permitted Use:	Restaurant	Restaurant

LEGAL IMPLICATIONS

This report and its recommendations are consistent with the following legislative provisions:

Local Government Act 2009
Local Government Regulation 2012
Retail Shop Leases Act 1994
Land Title Act 1994

POLICY IMPLICATIONS

The proposed lease terms are generally consistent with the Council's endorsed *Tenure over Council Property* policy (the 'Policy'). The only variation relates to the rent, which has been set at the current lease amount, adjusted by the Consumer Price Index (CPI) for the previous quarter, with a fixed annual escalation also based on CPI for the preceding quarter.

RISK MANAGEMENT IMPLICATIONS

Risks of Renewing the Lease for Five Years

1. Longer Term – Council have not considered renewing for longer than 5 years to allow further investigation and consideration of the future use of this building.

Risks of Alternative Recommendations

1. Shorter Lease Term – Offering a shorter lease term may provide flexibility but could result in frequent renegotiations and uncertainty for both parties.

Risks of Not Approving the Recommendation

1. Loss of Rental Income – If the lease is not renewed and no immediate alternative tenant is secured, then Council may face revenue loss due to property vacancy.
2. Community and Business Impact – Closure would diminish the vibrancy of the precinct and reduce community cohesion through inclusive dining experiences and charitable initiatives.

FINANCIAL/RESOURCE IMPLICATIONS

The current annual rent under the lease is $85,603.09 (excluding GST). The lessee is responsible for maintaining the premises in good repair throughout the term of the lease, except for fair wear and tear and replacement due to end-of-life deterioration.

COMMUNITY AND OTHER CONSULTATION

(a) Internal consultation was undertaken between the General Manager, Corporate Services; the General Manager, Community, Cultural and Economic Development; and Property Services to determine lease renewal terms that align with Council's strategic objectives and operational requirements.

(b) External engagement was led by the Chief Executive Officer and Matt Smith, General Manager (Corporate Services) who met with the current lessee, Mr Sharma, to discuss the renewal of the existing lease and his interest in a further term. Mr Sharma indicated a preference for a five-year term with a five-year renewal option.

However, in light of Council's future planning for the Arts Precinct, the Chief Executive Officer proposed a single five-year term without a renewal option was more suitable.

(c) The Chief Executive Officer has briefed the Mayor and Councillors on the proposed five-year lease term to be offered to Mr Sharma.

CONCLUSION

Renewing the lease for 116 Brisbane Street, Ipswich will maintain activation of a heritage-listed asset while providing Council with flexibility to plan for its future integration into the Arts Precinct. The recommended five-year term reflects strategic priorities and has received positive support through consultation. It is recommended that Council apply the relevant exception under the *Local Government Regulation 2012* to proceed with the lease renewal to Mr Sharma.

HUMAN RIGHTS IMPLICATIONS

HUMAN RIGHTS IMPACTS	
OTHER DECISION	
(a) What is the Act/Decision being made?	Recommendation A-C outlines Council will apply an exemption to dispose of a leasehold interest for the purpose of a restaurant.
(b) What human rights are affected?	Recognition and equality before the law (section 15) Protection from torture and cruel, inhuman or degrading treatment (section 17) Freedom of movement (section 19) Freedom of expression (section 21) Peaceful assembly and freedom of association (section 22) Privacy and reputation (section 25)
(c) How are the human rights limited?	The proposed decision to enter the lease will potentially interfere to restrict with the rights identified above because the lessee will have the power to eject persons in particular circumstances.
(d) Is there a good reason for limiting the relevant rights? Is the limitation fair and reasonable?	Yes. Ejecting a person in particular circumstances is a reasonable approach to ensure health and safety. Less restrictive means would be warnings, etc, but it is anticipated that these would be utilised prior to any ejection
(e) Conclusion	The decision is consistent with human rights.

ATTACHMENTS AND CONFIDENTIAL BACKGROUND PAPERS

1.	Title Search - 116 Brisbane Street, Ipswich ⇩
2.	Property Plan - Indian Mehfil Restaurant ⇩

Kerry Perrett
SENIOR PROPERTY OFFICER (TENURE)

I concur with the recommendations contained in this report.

Alicia Rieck
PROPERTY SERVICES MANAGER

I concur with the recommendations contained in this report.

Matt Smith
GENERAL MANAGER (CORPORATE SERVICES)

"Together, we proudly enhance the quality of life for our community"

INTERNAL CURRENT TITLE SEARCH
QUEENSLAND TITLES REGISTRY PTY LTD

Search Date: 17/09/2025 11:23 Title Reference: 50209132
Date Created: 02/03/1998

Previous Title: 16978016
16978017

REGISTERED OWNER

Dealing No: 702531098 26/02/1998

IPSWICH CITY COUNCIL

ESTATE AND LAND

Estate in Fee Simple

LOT 12 SURVEY PLAN 103223
Local Government: IPSWICH

EASEMENTS, ENCUMBRANCES AND INTERESTS

1. Rights and interests reserved to the Crown by
Deed of Grant No. 10188085 (ALLOT 11 SEC 5)
(ALLOT 22 SEC 5)
Deed of Grant No. 19565001 (ALLOT 23 SEC 5)
(ALLOT 10 SEC 5)

2. LEASE No 721502432 24/02/2022 at 10:49
RAJESH SHARMA
OF PART OF THE GROUND FLOOR (LEASE C)
TERM: 01/07/2021 TO 30/06/2026 OPTION NIL
Lodged at 10:49 on 24/02/2022 Recorded at 16:01 on 02/03/2022

ADMINISTRATIVE ADVICES

Dealing	Type	Lodgement Date	Status	Location
AS13964F	HERITGE SITE QUEENSLAND HERITAGE ACT 1992	09/09/1993 00:00	CUR	BE-ARCH -00
AS13965D	HERITGE SITE QUEENSLAND HERITAGE ACT 1992	09/09/1993 00:00	CUR	BE-ARCH -00
AS14035F	HERITGE SITE QUEENSLAND HERITAGE ACT 1992	10/09/1993 00:00	CUR	BE-ARCH -00

UNREGISTERED DEALINGS - NIL

Caution - Charges do not necessarily appear in order of priority

** End of Current Title Search **

Item 2 / Attachment 2.

Ipswich City Council
PO Box 191
IPSWICH QLD 4305
Australia

Telephone	(07) 3810 6666
Fax	(07) 3810 6731
Email	council@ipswich.qld.gov.au
Web	www.ipswich.qld.gov.au
Business Hours	8:00am - 4:30pm (Mon - Fri)

Property Plan - Indian Mehfil Restaurant

Scale 1:500
Metres
Metres 10 20 30

Printed Date: 19 Sep 2025

Doc ID No: A12013882

ITEM: 3

SUBJECT: INFORMATION AND CYBER SECURITY POLICY

AUTHOR: BUSINESS SUPPORT OFFICER

DATE: 16 SEPTEMBER 2025

EXECUTIVE SUMMARY

This is a report concerning the review and update of the Information and Cyber Security Policy.

RECOMMENDATION/S

That the Finance and Governance Committee approve the updated Information and Cyber Security Policy in accordance with the standard four-year development and improvement cycle as detailed in Attachment 3.

RELATED PARTIES

There is no declaration of conflicts of interest.

IFUTURE THEME

A Trusted and Leading Organisation

PURPOSE OF REPORT/BACKGROUND

The Information and Cyber Security Policy was due for review in December 2023. The Policy has been reviewed to improve clarity, readability and understanding and reflect improvements to Council's cyber maturity. There were several role references within the policy that were no longer applicable due to changes to branch structure; therefore, they have been updated to improve readability.

The roles and responsibilities have been updated to improve clarity. The name of the Policy has been updated to reflect the scope of Council's cyber security responsibilities. Key stakeholders have been added to the policy reflecting the cross departmental nature of cyber security and related documents have been updated to reflect the changing technology and policy landscape.

LEGAL IMPLICATIONS

This report and its recommendations are consistent with the following legislative provisions:
Local Government Act 2009

POLICY IMPLICATIONS

There are no policy implications.

RISK MANAGEMENT IMPLICATIONS

n/a

FINANCIAL/RESOURCE IMPLICATIONS

n/a

COMMUNITY AND OTHER CONSULTATION

Cyber Security Team
Cyber Security Project Manager
Infrastructure Lead
Service Delivery Lead
ICT Operations Manager
Chief Information Officer
Governance Services Team have been consulted during this review
Executive Leadership Team
Mayor and Councillors

CONCLUSION

That the updated Information and Cyber Security Policy be approved in accordance with the standard four-year development and improvement cycle.

HUMAN RIGHTS IMPLICATIONS

HUMAN RIGHTS IMPACTS	
NON-DISCRETIONARY DECISION	
Recommendation That the Finance and Governance Committee approve the updated Information and Cyber Security Policy in accordance with the standard four-year development and improvement cycle as detailed in Attachment 3. Therefore, while the proposed decision may not be compatible with human rights Council's decision will not be unlawful under the *Human Rights Act 2019*.	

ATTACHMENTS AND CONFIDENTIAL BACKGROUND PAPERS

1.	Policy - Information Systems Security (InfoSec) - ORIGINAL ⇩
2.	Policy - Information Systems Security (InfoSec) - TRACKED CHANGES ⇩
3.	Policy - Information and Cyber Security - CLEAN SKIN ⇩

Leanne Sherriff
BUSINESS SUPPORT OFFICER

I concur with the recommendations contained in this report.

Angela Jackson
CHIEF INFORMATION OFFICER

I concur with the recommendations contained in this report.

Matt Smith
GENERAL MANAGER (CORPORATE SERVICES)

"Together, we proudly enhance the quality of life for our community"

Information Systems Security (InfoSec) Policy

Collaboration Communication Integrity Efficiency Leadership

Version Control and Objective ID	Version No: 1	Objective ID: A5885002
Adopted at Council Ordinary Meeting on	10 December 2019	
Date of Review	10 December 2023	

1. Statement

Council will establish and maintain an Information Security Management System (ISMS) that provides for appropriate security and confidentiality of information, information systems, applications and networks owned, leased or operated by all Council users, operations and entities as required to address corporate risks and to satisfy regulatory requirements.

2. Purpose and Principles

This policy guides Council's approach to managing the security of all digital information captured in and managed by information systems used across council. The following principles and requirements underpin Council's commitment to InfoSec:

Policy Aspect	Requirement
Information Security Planning, Capability and Risk Management	Council will establish an Information Security Management System (ISMS), approved by the ICT Steering Committee, to manage Council's InfoSec risks. The ISMS will detail: a. InfoSec goals and strategic objectives of Council, including how InfoSec management intersects with and supports broader business objectives and priorities b. Threats, risks and vulnerabilities that impact the protection of Council's ICT Assets c. Council's tolerance to InfoSec related risks d. Council's capability and capacity to manage and develop InfoSec Controls e. Council's strategies to implement and maintain the ISMS, maintain a positive risk culture and deliver against this Policy.
ISMS Administration and Reporting	Matters relating to the routine operation, administration and evolution of Council's ISMS will be overseen by the Manager ICT Branch (CIO). ISMS matters requiring escalation will be taken, in the first instance, to the ICT Steering Committee for consideration and direction. InfoSec Risks will also be captured, reported and tracked within the Council's Risk Management Framework. The ICT Steering Committee will provide a bi-annual report on the ISMS to the Audit and Risk Committee on: a. The security outcomes supported by the ISMS b. The maturity of the capability identified in the InfoSec Framework c. Key risks to Council's ICT Assets d. Details of measures taken to mitigate or otherwise manage identified security risks
InfoSec Governance for Contracted Service Providers	The requirements of this Policy apply equally to ICT Assets procured directly or included indirectly as part of any broader outsourcing of business services. Each Business System Owner is accountable for the risks arising from ICT Assets procured as a component of broader business outsourcing.

IPSWICH CITY COUNCIL | Information Systems Security (InfoSec) Policy

Policy Aspect	Requirement
Sensitive and Classified Digital Information	Council will: a. Identify and classify Digital Information developed and used across Council for the purpose of defining and enforcing appropriate InfoSec Controls b. Assess the sensitivity and security classification of Digital Information holdings c. Implement proportional InfoSec Controls for Digital Information reflecting the value, importance and sensitivity
Proportional InfoSec Controls	Council will define and enforce InfoSec Controls based on the Risk exposure associated with the loss or compromise of any given ICT Resource. In determining InfoSec Controls to be applied Council will consider: a. **Confidentiality:** Risk associated with unauthorised access to any given ICT Resource and ensuring that ICT Resources are only accessible to those with authorised access b. **Integrity:** Risk associated with the accuracy and completeness of Digital Information and processing methods c. **Availability:** Risk associated with the loss of availability, or degraded performance of ICT Resources
Safeguarding Information from Threats	Council will, as a minimum, mitigate common and emerging InfoSec threats based on the Australian Cyber Security Centre "Essential Eight" controls: a. Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers. b. Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate. c. Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications. d. User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers. e. Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing. f. Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository. g. Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions. h. Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes. Council will adopt or extend further InfoSec Controls as necessary to safeguard information as informed via structured risk assessments.

Policy Aspect	Requirement
Access to ICT Resources	Council will enforce access controls to ICT Resources. This includes: a. Ensuring that System Users who access sensitive or classified Digital Information have appropriate authorisation and continuing need to access that Information b. Controlling access to supporting ICT Assets and Services (networks, remote access, infrastructure and applications etc), both on-premise and cloud hosted c. Periodic audit of System User access and activity to ensure appropriate and reasonable access to ICT Assets
InfoSec Controls Across ICT Asset Lifecycle	Council will ensure InfoSec Controls are properly considered, implemented and maintained across the operating lifecycle of all ICT Assets including: a. Sensitive and classified information is identified, and appropriate InfoSec requirements are addressed in the specifications, analysis and/or design phases for new ICT Assets b. Where the ICT Asset is procured 'as-a-service', all requirements of this policy are considered with required controls reflected in the service contract c. InfoSec Controls are established and validated during all stages of System development, as well as when new Systems are implemented and maintained in the operational environment d. Appropriate change control, acceptance and system testing, planning and migration control measures are carried out when upgrading or installing software in the operational environment e. A patch management program for operating systems, firmware and applications of all ICT Assets is implemented to maintain vendor support, increase stability and reduce the likelihood of threats being exploited

3. Strategic Plan Links

This policy aligns with the following iFuture 2021-2026 Corporate Plan themes:

- Vibrant and Growing
- A Trusted and Leading Organisation

4. Regulatory Authority

- QGCIO Information Security Policy (IS18:2018)
- Public Records Act 2002
- Right to Information Act 2009
- Information Privacy Act 2009
- Local Government Act 2009

5. Human Rights Commitment

Ipswich City Council (Council) has considered the human rights protected under the *Human Rights Act 2019 (Qld)* (the Act) when adopting and/or amending this policy. When applying this policy, Council will act and make decisions in a way that is compatible with human rights and give proper consideration to a human right relevant to the decision in accordance with the Act.

6. Scope

This Policy applies to internal Business System Owners, System Users and Risk Owners, not external customers and users of Council operated or supplied ICT Assets, Resources and Services.

External users (eg Citizens, Business etc) of Council's ICT Assets will be subject to terms and conditions unique to each offered service.

7. Roles and Responsibilities

Role	Responsibilities
Information Security Officer (ISO)	• Develop and maintain ISMS • Provide stakeholders with advice, guidance and services related to InfoSec • Review and approve InfoSec Controls for individual Information Assets • Establish, review, track and report on waivers and deviations issued against non-compliant Information Assets • Own and direct the development of InfoSec Controls the have enterprise applicability
ICT Strategy, Enterprise Architecture and Governance Manager	• Ensure appropriate governance across ISMS • Ensure coherent and structured architectural approach to InfoSec Controls
Manager ICT Branch (CIO)	• Owner of this Policy • Sponsor/owner of ISMS • Sponsorship and promotion of Governance of ISMS and InfoSec Risk Management
ICT Service Delivery Manager	• Routine operation and management of ICT Assets and InfoSec Controls
Records and Knowledge Manager	• Identify and classify Digital Information across all Council Information Assets • Review the Digital Information managed within any new ICT Asset undergoing procurement and implementation and provide advice to the Business Application Owner and the ISO on information sensitivity and security classification
Corporate Risk and Planning Manager	• Provide advice, interpretation and direction on InfoSec related risks and relevance/alignment with wider Council Risk Management Framework
ICT Steering Committee	• Review and provide advice and directions • Support/sponsor investment into InfoSec Controls required to achieve ISMS outcomes
Business System Owner	• Complying with this policy, the procedures, and applicable technical standards that extend on this Policy • Managing InfoSec risks associated with ICT resources and third party service providers under their remit; • Sponsoring and directing the development, implementation and maintenance of InfoSec Controls for ICT Assets under their remit, in accordance with the Risk Management Framework and applicable technical standards
System Users	• All System Users shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

8. Key Stakeholders

The following will be consulted during the review process:

- ICT Steering Committee
- Business System Owners

9. Monitoring and Evaluation

- Ageing and resolution of InfoSec related Departures and Waivers issued for non-compliant ICT Assets
- Effective identification and resolution of InfoSec Incidents as reported by SIEM
- Effective reporting and awareness of ISMS to both ICT Steering Committee and ARC
- Strategic and Operational Risks related to InfoSec exposure and Controls within tolerance
- Number of information security breaches related to non-compliance with ethical and professional behaviour guidelines
- Frequency of independent reviews of governance of information security
- Frequency of information security reporting to the ICT Steering committee
- Number of external/internal audits and reviews

10. Definitions

Term	Definition
Business System Owner	A person with primary accountability for the business outcomes and functions provided by a Council ICT Asset, including ownership and accountability for any associated InfoSec risk.
InfoSec	Information Security (InfoSec) is a set of related strategies, processes, tools and policies that collectively identify, classify, prevent, counter and recover from threats to ICT Resources.
InfoSec Control	Any contractual, management, operational or technical measure (including safeguards or countermeasures) put in place for the purpose of enabling and enforcing InfoSec.
InfoSec Incident	Any event that may adversely impact the confidentiality, integrity or availability of a Council ICT Resource.
Digital Information	Information that is in a digital or electronic form and is stored, processed or transmitted within an ICT Resource.
ICT	Information and Communications Technology that enables or supports Council owned or operated business, operating departments or services.
ICT Asset	Hardware, software, cloud-based services, communication devices, data centres, or networks that are owned, leased, leveraged or operated by Council.
ICT Resource	Any ICT Service, ICT Asset or Digital Information.
ICT Service	Any business or technology function provided using one or more ICT Assets, including, but not limited to: • application systems (including software-as-a-service); and • ICT infrastructure services such as operating systems, databases, voice and data telecommunications services, network services, media services, file and print services, and email services.
ISMS	An Information Security Management System (ISMS) is a cohesive and planned suite of policies, procedures, roles and InfoSec Controls for systematically protecting an organisation's ICT Resources. The goal of an ISMS is to minimise risk and ensure business continuity by pro-actively addressing known InfoSec risks and limiting the impact of any InfoSec Incident.
Risk	Has the meaning provided in the Risk Management Framework 2019.

System User	Any Council employee, volunteer, contractor or elected official that is provided with access to Council provided ICT Resources.

11. Policy Owner

The General Manager (Corporate Services) is the policy owner and the Chief Information Officer (ICT) is responsible for authoring and reviewing this policy.

Information and Cyber ~~Systems~~ Security ~~(InfoSec)~~ Policy

Collaboration Communication Integrity Efficiency Leadership

Version Control and Objective ID	Version No: 1.1	Objective ID: A5885002
Adopted at Council Ordinary Meeting on	~~10 December 2019~~	
Date of Review	~~10 December 2023~~	

1. Statement

Council will establish and maintain an Information Security Management System (ISMS) that aligns with security industry best practices and provides for appropriate security ~~and confidentiality~~ of information, information systems, ICT services and assets ~~applications and networks owned, leased or operated by all Council users, operations and entities~~ as required to address information and cyber ~~corporate~~ risks, and to satisfy regulatory requirements.

2. Purpose and Principles

The Information Security Management System (ISMS), refers to a framework of:

- Policy, Administrative Directive, Procedures, and supporting documents.
- Technological controls, ICT and Governance processes.
- Security awareness training and education for Council Users

for systematically ensuring security is applied and continuously improved to address risks to information assets, and Council's compliance obligations.

The ISMS will be based on the following principles:

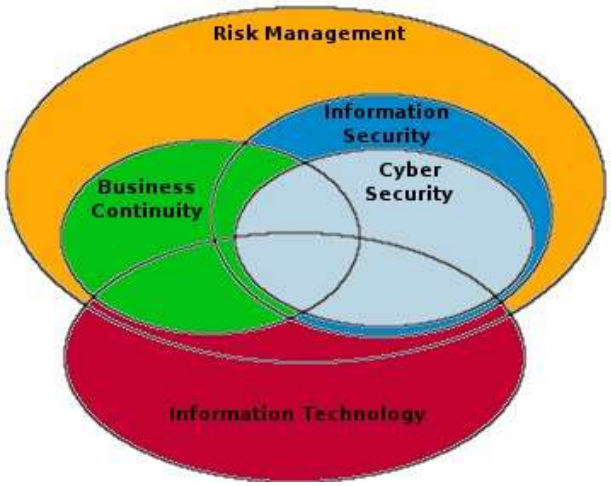
- Defence-in-depth (Layered Security / no single point of failure).
- Least privileges (need-to-know / need-to-have).
- Segregation of duties (no single point of complete control).
- Secure by design (from Initiatives through SDLC to production).
- Enhanced corporate resilience (withstand and recover from security incidents and disruptions).

An effective ISMS will:

- Ensure the Confidentiality, Integrity, and Availability of information – Information Security.
- Defend against cyber-attacks (e.g. hacking, malware, phishing, etc) targeting ICT systems, networks, and digital data – Cyber Security.
- Maintain the security of Council information during its lifecycle.
- Protect Ipswich City Council brand and reputation.
- Ensure compliance with relevant regulatory, legal, and contractual requirements.

IPSWICH CITY COUNCIL | Information ~~Systems~~and Cyber Security ~~(InfoSec)~~ Policy

Relationships between Information Security, Cyber Security, Risk Management, BCP:



~~This policy guides Council's approach to managing the security of all digital information captured in and managed by information systems used across council. The following principles and requirements underpin Council's commitment to InfoSec:~~

~~Policy Aspect~~	~~Requirement~~
~~Information Security Planning, Capability and Risk Management~~	~~Council will establish an Information Security Management System (ISMS), approved by the ICT Steering Committee, to manage Council's InfoSec risks. The ISMS will detail:~~ ~~a. InfoSec goals and strategic objectives of Council, including how InfoSec management intersects with and supports broader business objectives and priorities~~ ~~b. Threats, risks and vulnerabilities that impact the protection of Council's ICT Assets~~ ~~c. Council's tolerance to InfoSec related risks~~ ~~d. Council's capability and capacity to manage and develop InfoSec Controls~~ ~~e.~~a. ~~Council's strategies to implement and maintain the ISMS, maintain a positive risk culture and deliver against this Policy.~~
~~ISMS Administration and Reporting~~	~~Matters relating to the routine operation, administration and evolution of Council's ISMS will be overseen by the Manager ICT Branch (CIO).~~ ~~ISMS matters requiring escalation will be taken, in the first instance, to the ICT Steering Committee for consideration and direction. InfoSec Risks will also be captured, reported and tracked within the Council's Risk Management Framework.~~ ~~The ICT Steering Committee will provide a bi-annual report on the ISMS to the Audit and Risk Committee on:~~ ~~a. The security outcomes supported by the ISMS~~ ~~b. The maturity of the capability identified in the InfoSec Framework~~ ~~c. Key risks to Council's ICT Assets~~ ~~d.~~b. ~~Details of measures taken to mitigate or otherwise manage identified security risks~~
~~InfoSec Governance for Contracted Service Providers~~	~~The requirements of this Policy apply equally to ICT Assets procured directly or included indirectly as part of any broader outsourcing of business services.~~ ~~Each Business System Owner is accountable for the risks arising from ICT Assets procured as a component of broader business outsourcing.~~

IPSWICH CITY COUNCIL | Information ~~Systems~~and Cyber Security ~~(InfoSec)~~ Policy

~~Policy Aspect~~	~~Requirement~~
~~**Sensitive and Classified Digital Information**~~	~~Council will:~~ ~~a. Identify and classify Digital Information developed and used across Council for the purpose of defining and enforcing appropriate InfoSec Controls~~ ~~b. Assess the sensitivity and security classification of Digital Information holdings~~ c. ~~Implement proportional InfoSec Controls for Digital Information reflecting the value, importance and sensitivity~~
~~**Proportional InfoSec Controls**~~	~~Council will define and enforce InfoSec Controls based on the Risk exposure associated with the loss or compromise of any given ICT Resource. In determining InfoSec Controls to be applied Council will consider:~~ ~~a. **Confidentiality:** Risk associated with unauthorised access to any given ICT Resource and ensuring that ICT Resources are only accessible to those with authorised access~~ ~~b. **Integrity:** Risk associated with the accuracy and completeness of Digital Information and processing methods~~ ~~c.~~d. ~~**Availability:** Risk associated with the loss of availability, or degraded performance of ICT Resources~~
~~**Safeguarding Information from Threats**~~	~~Council will, as a minimum, mitigate common and emerging InfoSec threats based on the Australian Cyber Security Centre "Essential Eight" controls:~~ ~~a. Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.~~ ~~b. Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.~~ ~~c. Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.~~ ~~d. User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.~~ ~~e. Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.~~ ~~f. Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high availability) data repository.~~ ~~g. Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.~~ ~~h. Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.~~ ~~Council will adopt or extend further InfoSec Controls as necessary to safeguard information as informed via structured risk assessments.~~

~~Policy Aspect~~	~~Requirement~~
~~Access to ICT Resources~~	~~Council will enforce access controls to ICT Resources. This includes:~~ ~~a. Ensuring that System Users who access sensitive or classified Digital Information have appropriate authorisation and continuing need to access that Information~~ ~~b. Controlling access to supporting ICT Assets and Services (networks, remote access, infrastructure and applications etc), both on-premise and cloud hosted~~ ~~c.~~e. ~~Periodic audit of System User access and activity to ensure appropriate and reasonable access to ICT Assets~~
~~InfoSec Controls Across ICT Asset Lifecycle~~	~~Council will ensure InfoSec Controls are properly considered, implemented and maintained across the operating lifecycle of all ICT Assets including:~~ ~~a. Sensitive and classified information is identified, and appropriate InfoSec requirements are addressed in the specifications, analysis and/or design phases for new ICT Assets~~ ~~b. Where the ICT Asset is procured 'as-a-service', all requirements of this policy are considered with required controls reflected in the service contract~~ ~~c. InfoSec Controls are established and validated during all stages of System development, as well as when new Systems are implemented and maintained in the operational environment~~ ~~d. Appropriate change control, acceptance and system testing, planning and migration control measures are carried out when upgrading or installing software in the operational environment~~ ~~e.~~f. ~~A patch management program for operating systems, firmware and applications of all ICT Assets is implemented to maintain vendor support, increase stability and reduce the likelihood of threats being exploited~~

3. Strategic Plan Links

This policy aligns with the following iFuture 2021-2026 Corporate Plan themes:

- Vibrant and Growing
- A Trusted and Leading Organisation

4. Regulatory Authority

- QGCIO Information and Cyber Security Policy (IS18:20~~18~~25)
- Public Records Act 2002
- Right to Information Act 2009
- Information Privacy Act 2009
- Local Government Act 2009

5. Human Rights Commitment

Ipswich City Council (Council) has considered the human rights protected under the *Human Rights Act 2019 (Qld)* (the Act) when adopting and/or amending this policy. When applying this policy, Council will act and make decisions in a way that is compatible with human rights and give proper consideration to a human right relevant to the decision in accordance with the Act.

6. Scope

This policy applies to all employees of Council, Councillors, and contractors regardless of whether they are permanent, temporary, fulltime, part-time, casual employees or volunteers – who have access or interaction with Council digital information and the ICT systems it is created, managed, or stored in.

~~This Policy applies to internal Business System Owners, System Users and Risk Owners, not external customers and users of Council operated or supplied ICT Assets, Resources and Services.~~

~~External users (eg Citizens, Business etc) of Council's ICT Assets will be subject to terms and conditions unique to each offered service.~~

7. Roles and Responsibilities

As per Scope, everyone at Council has responsibility and accountability in relation to information security in different forms and levels:

- Councillors, CEO and Executive Leadership Team – Top level accountability for Council's information security, its endorsement, support, and integration in corporate strategies.
- Business System Owners and Managers – Contribute to and ensure compliance with information security requirements and objectives.
- System Users – Aware and comply with information security requirements.
- ICT Branch – Advise, implement, and maintain the ISMS requirements and its continuous improvement.

Key roles and responsibilities for information security are further detailed in the Information Security Administrative Directive and defined in other documents supporting this policy including Security Standards and Procedures.

~~Role~~	~~Responsibilities~~
~~Information Security Officer (ISO)~~	~~• Develop and maintain ISMS~~ ~~• Provide stakeholders with advice, guidance and services related to InfoSec~~ ~~• Review and approve InfoSec Controls for individual Information Assets~~ ~~• Establish, review, track and report on waivers and deviations issued against non-compliant Information Assets~~ ~~• Own and direct the development of InfoSec Controls the have enterprise applicability~~
~~ICT Strategy, Enterprise Architecture and Governance Manager~~	~~• Ensure appropriate governance across ISMS~~ ~~• Ensure coherent and structured architectural approach to InfoSec Controls~~
~~Manager ICT Branch (CIO)~~	~~• Owner of this Policy~~ ~~• Sponsor/owner of ISMS~~ ~~• Sponsorship and promotion of Governance of ISMS and InfoSec Risk Management~~
~~ICT Service Delivery Manager~~	~~• Routine operation and management of ICT Assets and InfoSec Controls~~

~~Role~~	~~Responsibilities~~
~~**Records and Knowledge Manager**~~	• ~~Identify and classify Digital Information across all Council Information Assets~~ • ~~Review the Digital Information managed within any new ICT Asset undergoing procurement and implementation and provide advice to the Business Application Owner and the ISO on information sensitivity and security classification~~
~~**Corporate Risk and Planning Manager**~~	• ~~Provide advice, interpretation and direction on InfoSec related risks and relevance/alignment with wider Council Risk Management Framework~~
~~**ICT Steering Committee**~~	• ~~Review and provide advice and directions~~ • ~~Support/sponsor investment into InfoSec Controls required to achieve ISMS outcomes~~
~~**Business System Owner**~~	• ~~Complying with this policy, the procedures, and applicable technical standards that extend on this Policy~~ • ~~Managing InfoSec risks associated with ICT resources and third party service providers under their remit;~~ • ~~Sponsoring and directing the development, implementation and maintenance of InfoSec Controls for ICT Assets under their remit, in accordance with the Risk Management Framework and applicable technical standards~~
~~**System Users**~~	• ~~All System Users shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.~~

8. Key Stakeholders

~~The following will be consulted during the review process:~~

- ICT Steering Committee
- CEO and General Managers
- ~~Business System Owners~~
- Corporate Services Division
- Internal Audit

9. Monitoring and Evaluation

This policy will be reviewed in accordance with Council's policy review cycle or sooner as required by significance changes in government regulations, legislations, or the security threat landscape.

- ~~Ageing and resolution of InfoSec related Departures and Waivers issued for non-compliant ICT Assets~~
- ~~Effective identification and resolution of InfoSec Incidents as reported by SIEM~~
- ~~Effective reporting and awareness of ISMS to both ICT Steering Committee and ARC~~
- ~~Strategic and Operational Risks related to InfoSec exposure and Controls within tolerance~~
- ~~Number of information security breaches related to non-compliance with ethical and professional behaviour guidelines~~
- ~~Frequency of independent reviews of governance of information security~~
- ~~Frequency of information security reporting to the ICT Steering committee~~
- ~~Number of external/internal audits and reviews~~

10. ~~Definitions~~

~~Term~~	~~Definition~~
~~Business System Owner~~	~~A person with primary accountability for the business outcomes and functions provided by a Council ICT Asset, including ownership and accountability for any associated InfoSec risk.~~
~~InfoSec~~	~~Information Security (InfoSec) is a set of related strategies, processes, tools and policies that collectively identify, classify, prevent, counter and recover from threats to ICT Resources.~~
~~InfoSec Control~~	~~Any contractual, management, operational or technical measure (including safeguards or countermeasures) put in place for the purpose of enabling and enforcing InfoSec.~~
~~InfoSec Incident~~	~~Any event that may adversely impact the confidentiality, integrity or availability of a Council ICT Resource.~~
~~Digital Information~~	~~Information that is in a digital or electronic form and is stored, processed or transmitted within an ICT Resource.~~
~~ICT~~	~~Information and Communications Technology that enables or supports Council owned or operated business, operating departments or services.~~
~~ICT Asset~~	~~Hardware, software, cloud-based services, communication devices, data centres, or networks that are owned, leased, leveraged or operated by Council.~~
~~ICT Resource~~	~~Any ICT Service, ICT Asset or Digital Information.~~
~~ICT Service~~	~~Any business or technology function provided using one or more ICT Assets, including, but not limited to:~~ ~~• application systems (including software-as-a-service); and~~ ~~• ICT infrastructure services such as operating systems, databases, voice and data telecommunications services, network services, media services, file and print services, and email services.~~
~~ISMS~~	~~An Information Security Management System (ISMS) is a cohesive and planned suite of policies, procedures, roles and InfoSec Controls for systematically protecting an organisation's ICT Resources. The goal of an ISMS is to minimise risk and ensure business continuity by pro-actively addressing known InfoSec risks and limiting the impact of any InfoSec Incident.~~
~~Risk~~	~~Has the meaning provided in the Risk Management Framework 2019.~~
~~System User~~	~~Any Council employee, volunteer, contractor or elected official that is provided with access to Council provided ICT Resources.~~

11. Related Documents

Information Governance Policy

Information Privacy Policy

Record Keeping Policy

Artificial Intelligence Policy

Information Security Administrative Directive

ICT Acceptable Use Administrative Directive

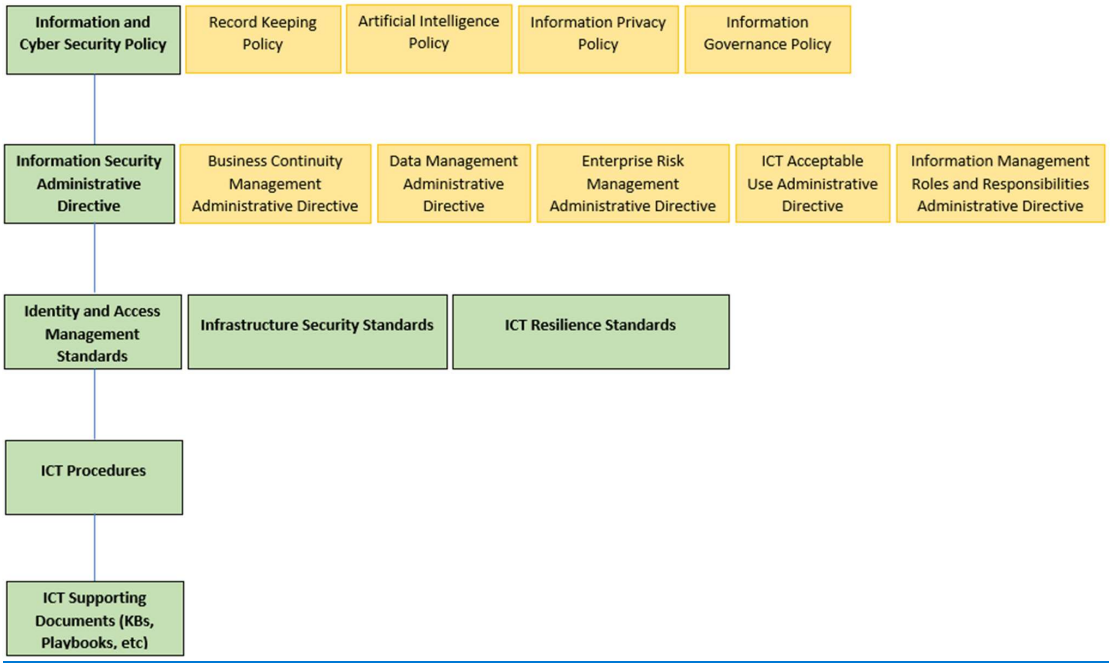
Data Management Administrative Directive

Enterprise Risk Management Administrative Directive

Business Continuity Management Administrative Directive

Information Management Roles and Responsibilities Administrative Directive

The Information Security policy document suite is as follows:



12. Policy Owner

The General Manager (Corporate Services) is the policy owner and the Chief Information Officer (ICT) is responsible for authoring and reviewing this policy.

Information and Cyber Security Policy

Safety and Wellbeing | Collaboration | Communication | Integrity | Efficiency | Leadership

Version Control and Objective ID	Version No: 2	Objective ID: A5885002
Adopted at Council Ordinary Meeting on		
Date of Review		

1. Statement

Council will establish and maintain an Information Security Management System (ISMS) that aligns with security industry best practices and provides for appropriate security of information, information systems, ICT services and assets as required to address information and cyber risks, and to satisfy regulatory requirements.

2. Purpose and Principles

The Information Security Management System (ISMS), refers to a framework of:

- Policy, Administrative Directive, Procedures, and supporting documents.
- Technological controls, ICT and Governance processes.
- Security awareness training and education for Council Users

for systematically ensuring security is applied and continuously improved to address risks to information assets, and Council's compliance obligations.

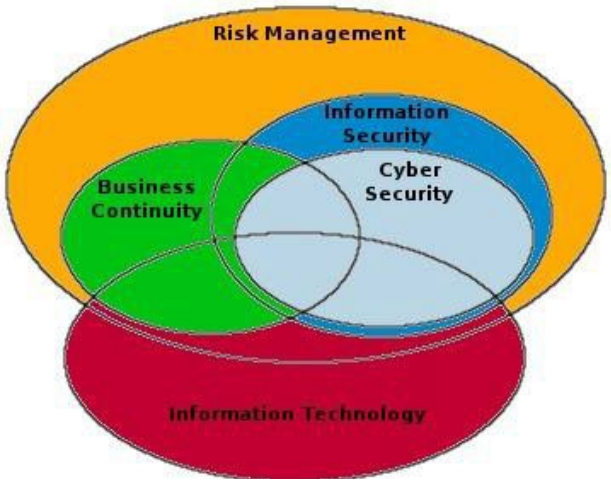
The ISMS will be based on the following principles:

- Defence-in-depth (Layered Security / no single point of failure).
- Least privileges (need-to-know / need-to-have).
- Segregation of duties (no single point of complete control).
- Secure by design (from Initiatives through Software Development Life Cycle to production).
- Enhanced corporate resilience (withstand and recover from security incidents and disruptions).

An effective ISMS will:

- Ensure the Confidentiality, Integrity, and Availability of information – Information Security.
- Defend against cyber-attacks (e.g. hacking, malware, phishing, etc) targeting ICT systems, networks, and digital data – Cyber Security.
- Maintain the security of Council information during its lifecycle.
- Protect Ipswich City Council brand and reputation.
- Ensure compliance with relevant regulatory, legal, and contractual requirements.

Relationships between Information Security, Cyber Security, Risk Management, BCP:



3. Strategic Plan Links

This policy aligns with the following iFuture 2021-2026 Corporate Plan themes:

- Vibrant and Growing
- A Trusted and Leading Organisation

4. Regulatory Authority

- QGCIO Information and Cyber Security Policy (IS18:2025)
- Public Records Act 2002
- Right to Information Act 2009
- Information Privacy Act 2009
- Local Government Act 2009

5. Human Rights Commitment

Ipswich City Council (Council) has considered the human rights protected under the *Human Rights Act 2019 (Qld)* (the Act) when adopting and/or amending this policy. When applying this policy, Council will act and make decisions in a way that is compatible with human rights and give proper consideration to a human right relevant to the decision in accordance with the Act.

6. Scope

This policy applies to all employees of Council, Councillors, and contractors regardless of whether they are permanent, temporary, fulltime, part-time, casual employees or volunteers who have access or interaction with Council digital information and the ICT systems it is created, managed, or stored in.

7. Roles and Responsibilities

As per Scope, everyone at Council has responsibility and accountability in relation to information security in different forms and levels:

- The Councillors, Chief Executive Officer, and Executive Leadership Team collectively share responsibility for Council's information security by ensuring its endorsement, support, and integration within corporate strategies.
- Business System Owners and Managers – Contribute to and ensure compliance with information security requirements and objectives.
- System Users – Aware and comply with information security requirements.
- ICT Branch – Advise, implement, and maintain the ISMS requirements and its continuous improvement.

Key roles and responsibilities for information security are further detailed in the Information Security Administrative Directive and defined in other documents supporting this policy including Security Standards and Procedures.

8. Key Stakeholders

- ICT Steering Committee
- CEO and General Managers
- Corporate Services Division
- Internal Audit

9. Monitoring and Evaluation

This policy will be reviewed in accordance with Council's policy review cycle or sooner as required by significance changes in government regulations, legislations, or the security threat landscape.

10. Related Documents

Information Governance Policy

Information Privacy Policy

Record Keeping Policy

Artificial Intelligence Policy

Information Security Administrative Directive

ICT Acceptable Use Administrative Directive

Data Management Administrative Directive

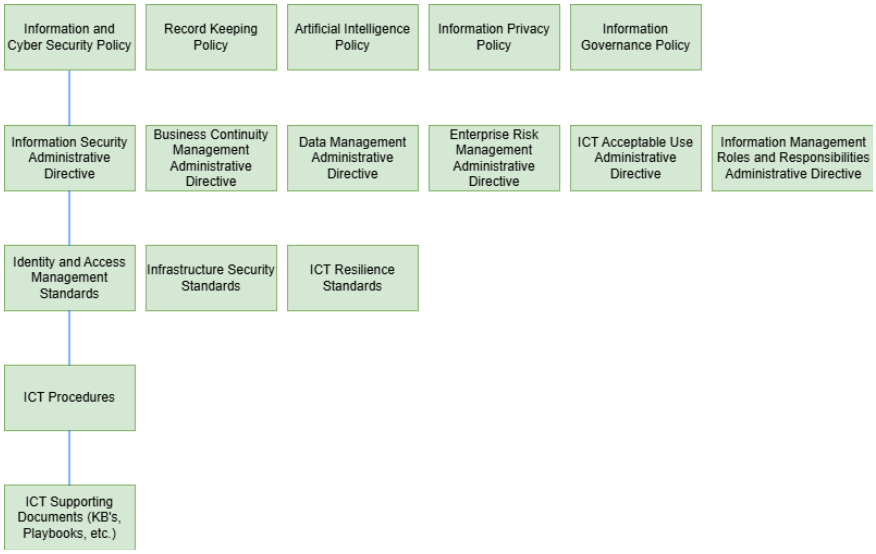
Enterprise Risk Management Administrative Directive

Business Continuity Management Administrative Directive

Information Management Roles and Responsibilities Administrative Directive

IPSWICH CITY COUNCIL | Information and Cyber Security Policy

The Information Security policy document suite is as follows:



11. Policy Owner

The General Manager (Corporate Services) is the policy owner and the Chief Information Officer (ICT) is responsible for authoring and reviewing this policy.