

Name of policy:	Records and Information Management		
Adoption by Council:	29 April 2026	Minute number:	2026/116
Last review date:	29 April 2026		
Review timeframe:	Two years (to align with the RMA assessment timeframe)		
Next scheduled review date:	29 April 2028		
Related legislation:	• <i>State Records Act 1998</i> • <i>State Records Regulation 2024 (NSW)</i> • <i>Standard No. 15 – Standard on records management (2025)</i> • <i>Standard No. 14 – Physical Storage of State Records (2025)</i> • <i>State Records Retention & Disposal Authorities: FA450 (Local Government), GA28 (Administrative), GA51 (Original/Source Records That Have Been Copied), GA48 (Source Records That Have Been Migrated), FA428 (Cemeteries and Crematoria Operations), FA367 (Water Supply and Wastewater Management)</i> • <i>Government Information (Public Access) Act 2009 (GIPA)</i> • <i>Privacy and Personal Information Protection Act 1998 (PPIPA)</i> • <i>Health Records and Information Privacy Act 2002 (HRIPA)</i> • <i>Environmental Planning and Assessment Act 1979</i> • <i>NSW Cyber Security Policy; Cyber Security Guidelines – Local Government (OLG/Cyber Security NSW)</i> • <i>NSW Government Information Classification, Labelling & Handling Guidelines (Data.NSW)</i> • <i>NSW Government Open Data Policy (and IPC GIPA guidance)</i> • <i>ISO/IEC 29151 (informative guidance for controls relating to personally identifiable information)</i>		

Associated policies/documents:	• Code of Conduct • Information Management Framework • ICT Strategy • Privacy Management Plan • Digitisation Guideline (GA51 compliance) • Off-site Storage Guidelines • Cyber Incident Response Plan & Public Data Breach Policy • Social Media Policy and Guidelines • Data Governance Toolkit (Data.NSW) • Disposal and Destruction of Records Procedure
Responsible division:	Corporate Services

Policy objective

To ensure full and accurate records of all activities and decisions are created, captured, protected, managed, used, retained, disposed of, or transferred in accordance with NSW recordkeeping legislation and standards - enabling transparency, accountability, efficient service delivery, good governance, and public trust. This policy also ensures that Council's information assets are securely stored, efficiently organised, and appropriately accessed across approved repositories.

Council is committed to meeting its responsibilities under the Act by implementing best practices in records and information management and will endeavour to comply (where possible) with the relevant legislation.

Policy statement

Council recognises records, information and data as strategic assets. Council will manage them across the full lifecycle, including; creation, capture, use/access, storage, retention, and disposal or transfer to State Archives so they remain authentic, reliable, usable and accessible for as long as required, and appropriately secured against loss, misuse or unauthorised access. Records and information governance will be embedded in business processes, systems and service arrangements, including outsourced and cloud services.

Policy coverage

This policy and associated procedures apply to all Council officials (staff, Councillors, contractors, volunteers) and to all formats of records and information (digital, physical, email, messaging, audiovisual, websites/social media, collaboration tools, and structured business systems), including those created or held by service providers (cloud, outsourced or shared services).

Strategic Plan link

Community Outcome: Leadership

L-3 – Provide open and transparent leadership with a focus on clear decision-making processes and ongoing communication with the community

Community Outcome: Leadership

L-4 – Deliver services to the community with a focus on customer service, efficiency, continuous improvement and long-term financial health

Policy content

1. Principles

- Governance & accountability: Council will maintain a coordinated set of policies, procedures, people, systems and activities to meet legislative obligations and business needs.
- Business enablement: Records, information and data required for council business will be identified and governed so systems can ensure its creation, capture, maintenance, usability and sustainability.
- Trustworthiness & protection: Records, information and data will be accurate, complete, secure and accessible, with authorised disposal only and long-term value preserved.
- Systems: Business and recordkeeping systems automatically create, capture and store records as part of standard business processes.
- Disposal and destruction: Records will be systematic, accountable, authorised and legally appropriate.

2. Governance & Responsibilities

General Manager

- Has delegated authority and ensures organisational compliance with the State Records Act and Regulation.
- Approves the Records & Information Management Program and resources.

Director Corporate Services — Senior Responsible Officer (SRO)

- Provides executive oversight of information governance.
- Notifies State Records NSW of damaged, lost or breached records where required.
- Authorises disposals, migrations and decommissioning.
- Leads the Records Management Assessment (RMAT)
- Ensures alignment with Cyber Security NSW and Data.NSW frameworks across records, privacy and security.

Manager Governance — Corporate Records Manager

- Maintains policy, procedures and training; oversees digitisation and GA51-compliant.
- Approves storage facilities, access directions and transfer plans to State Archives.
- Oversees the Records Management Assessment (RMAT) self-assessments and disposal processes.
- Partners with ICT/Security to embed Data.NSW classification/handling and Standard No. 15 controls.
- Ensures preservation of evidence and sentencing decisions post-incident.

Manager Information Technology

- Ensures the Electronic Document Management System (EDRMS), Enterprise Content Management (ECM) and other systems support capture, metadata, retention, access controls and export capability.
- Leads cyber incident response; maintains security controls and monitoring consistent with the NSW Cyber Security Policy and Local Government Guidelines.
- Coordinates with Manager Governance to protect records and metadata.
- Oversees Records Management Assessment (RMAT)
- Oversees the Information Asset Register and high-risk/high-value (HRHV) information risk treatment.
- Undertakes Disposal Processing of information

Information Management Teams

- Capture, classify and sentence records within corporate systems.
- Manage storage, retrieval, off-site transfers and audits.
- Provide training and education, and undertake digitising projects.
- Complete disposal documentation and quality control through implementing GA51.
- Source documents and information for staff and customers.

System Owners & Information Custodians

- Ensure recordkeeping requirements are built into system design and processes (capture, metadata, retention, access, export).
- Establish and maintain the repository structure and permissions in their domain.
- Ensure disposal holds are applied where necessary and participate in disposal approvals.

Council Officials

- Make and keep full and accurate records of Council business (emails, notes, letters, meetings, social media, working papers, drafts).
- Capture emails and other communications into the ECM/EDRMS or designated systems. Councillors ensure all records of Council business are captured in Council's corporate email system.

- Protect information and report incidents (loss, suspected loss or unauthorised disclosure) immediately to their manager.

3. Mandatory Requirements

Create & Capture

- Create and capture adequate records of decisions, approvals, commitments, business activities, communications and advice as soon as practicable into approved recordkeeping systems in line with Council's policies and procedures.

Approved Systems & Locations

- Store records only in approved systems – ECM is the approved EDMS.
- Do not use personal drives, USBs, private cloud accounts, or uncontrolled collaboration spaces to store official records.

Metadata & Context

- Maintain sufficient metadata (creator, date, function, approvals, relationships, version) so records remain understandable and usable over time.
- Precise descriptions are required to contain the legal title of a document or provide contextual and content information.

Access, Security & Privacy

- Manage access in line with authorisations, classification, security protocols and legislation (*Government Information (Public Access) Act 2009* (GIPA), *Privacy and Personal Information Protection Act 1998* (PPIPA) / *Health Records and Information Privacy Act 2002* (HRIPA), legal professional privilege).

Storage (Digital & Physical)

- Storage environments must maintain the integrity, authenticity and accessibility of records for as long as required.

Retention & Authorised Disposal

- Retain records per current authorised Retention & Disposal Authorities (e.g., FA450, GA28, GA51, GA48, FA428, FA367).
- Disposal must be justified, authorised, documented and auditable.
- Disposal and destruction of records will be systematic, accountable, authorised and legally appropriate. Refer to the Disposal and Destruction of Records Procedure.

Technology-Dependent Records (Digital Continuity)

- Ensure long-term accessibility via planned migration, format management and system succession planning.

System Changes & Decommissioning

- Before decommissioning a system, sentence all records; retain, migrate or dispose of them in line with RDAs; document all actions.

Transfer to State Archives

- Transfer records sentenced as State archives when no longer required for business use, in accordance with approved access directions.

Outsourced, Cloud & Service Arrangements

- All external service arrangements must explicitly address custody, control, ownership, access, retention, disposal, return/transfer, security, audit/assurance, NSW jurisdiction and incident response.
- See **Annexure A** for the mandatory due-diligence/contract checklist (including ISO/IEC 29151 alignment for PII).

Cyber Incidents & Data Breaches (MNDB Scheme)

- Adhere to the Mandatory Notification of Data Breaches (MNDB) scheme and Cyber Security NSW protocols: immediate containment, assess for “serious harm” within 30 days, notify the Information and Privacy Commission NSW and affected individuals as required, and maintain a breach register.
- Any suspected or confirmed cyber incident or data breach affecting the availability, integrity or confidentiality of Council records and information (including third-party hosted systems) must be treated as a recordkeeping incident and managed under the Cyber Incident Response Plan.
- Users must immediately notify their manager if confidential or sensitive information is lost, suspected lost, or disclosed to unauthorised parties.

Open Data & Public Access

- Data and information should be made publicly available where appropriate unless restricted for reasons of privacy, public safety, security, law enforcement, public health, or legal compliance.
- Use standard programs and formats for storing information and data so it is easily accessed, understood, modified and combined by different software applications.
- Public release requires classification as open access information or approval by a Director; where applicable, a Data Licence Agreement must be completed in line with the NSW Open Data Policy and IPC guidance.

4. Operational Requirements (User-Level Controls)

Repository structures

- Only authorised Information Custodians may update configuration of our Records and Information Management Systems.

Local and portable storage

- Do not save official information to local device storage or USB as the primary location.
- If a working copy is made locally/portable, ensure the authoritative copy is stored in an approved repository.
- Portable media reused within Council must be securely erased prior to reuse; media sent externally must be new or securely erased.

Protect information

- Electronic information must be protected based on its sensitivity, value, and criticality, regardless of the storage device, its location, the systems used to process it, or the processes it is subjected to, including the use of GenAI, Large Language Models

(LLMs), embedded AI or third party AI systems and tools to collect, create or modify the data or information.

- Staff should be trained to recognise information that should be classified, especially when it personally identifies individuals
- Lock screen when leaving device for a period of time

Creation of Records

- Data, information and records created, modified, saved, transmitted, or archived using systems owned or managed by MCC remains the property of MCC.
- Data and information collected, created or modified by GenAI, LLMs, embedded AI or third-party AI systems and tools must be checked for accuracy, bias, and reliability.

Passwords on documents/folders

- Do not apply passwords at document or folder level unless approved by the Information Technology Manager; if approved, store the password in an appropriate Council-managed repository.

Appropriate use & least privilege

- Do not browse Council systems out of curiosity; access only what is required for business purposes and what your permissions allow.

Printing, scanning and copying confidential information

- The authorised user must be present at the device during the process; use secure devices/locations with release-on-present (PIN/card).
- Take care to avoid sending information to the wrong recipient.

Digital signatures

- Use only in conjunction with an approved Digital Signature Management System.

Verbal sharing (classification first)

- Identify the classification before discussing sensitive information (in person or by phone); follow approved information management processes.

Remote working

- Use Council-approved equipment and storage; remove sensitive information from whiteboards/displays when no longer required.

Third-party transfers (physical or electronic)

- Protect information in transit; mark packages/file transfers clearly for the authorised recipient.
- Maintain a transfer log (see Annexure B) recording: media type; identifying numbers (e.g., serial/asset ID); recipient; description of information; and purpose of transfer.

5. Monitoring & Assurance

- Conduct regular reviews, health checks, audits and RMA self-assessments to ensure compliance.
- Test/audit systems routinely to ensure integrity, usability and accessibility are not compromised.

6. Training & Awareness

- All staff must complete induction and refresher training.
- Roles managing HRHV information/systems and Information Custodians require additional role-based training.

7. Non-Compliance

- Council applies corrective actions and continuous improvement where issues are identified.
- Non-compliance may lead to escalation to the SRO, mandatory reporting to relevant agencies, and disciplinary action in accordance with the Code of Conduct.

Definitions

Archives: Records identified as having continuing value and kept permanently as part of Council Archives.

Council: MidCoast Council.

Council Correspondence: Any document created for Council business (emails, notes, letters, meetings, social media, working papers, drafts).

Digital Records: Records communicated and maintained electronically.

ECM/EDRMS: Enterprise Content Management / Electronic Document & Records Management System (Council's corporate records system).

High-risk/High-value (HRHV) information: Information with significant operational, legal, financial, personal, regulatory or community impact if compromised, lost or inaccessible.

Record: Any document or source of information compiled, recorded or stored in any form in the course of Council business (per the State Records Act 1998).

Recordkeeping system: A system approved for creation, capture, management, storage, protection and retrieval of Council records.

Information Custodian: An individual or group designated by Council to oversee the management, structure, security, permissions and compliance of specific information repositories or datasets.

Information repositories: Systems or databases in which Council stores information, including approved cloud storage or other designated secure platforms.

Personally Identifiable Information (PII): Any data that can identify an individual (e.g., name, address, phone number, identifiers).

State record: A record made or received in the course of Council business.

References and related documents

Internal processes for staff are available on the intranet for example Information Technology Security and Disposal and Destruction of Records.

Responsible officer (position)

Manager Governance (Corporate Records Manager), and
Manager Information Technology

Annexure A — AU Third Party Cyber Risk Management Questionnaire

Supplier Security Audit	
Supplier Business Information	Supplier responses
Business Name:	
ABN/ACN:	
Respondent Name	
Respondent Contact Number	
Respondent Contact Email	
Date Submitted	
Company Online Presence	
Business Web Domain	
Service Web Domain	If different from above:
Is your service hosted within Australia?	
Is your customer information hosted or stored within Australia?	
Supplier Security Audit - Information Security and Governance	Supplier responses
Will/could the Supplier create, access, store, process, transfer, or destroy agency information/data in any manner?	
How does the supplier interact with or store information? Access only/IaaS, PaaS, SaaS, supplier hosted application, on-premises application, Commercial Off-The-Shelf (COTS) software, Custom developed software, Open source software, Mobile software, Other (If other, please explain).	
Will/could the Supplier have/receive administrator and/or privileged access to computer systems that create, access, store, process, or transfer Confidential or Protected information at any time?	
What is the sensitivity (or classification) of information created, accessed, stored, transferred, or destroyed by this Supplier?	
Does the supplier have access to or host Personally Identifiable Information owned by the agency?	
Please explain the geographic locations where Agency's data storage, transmission and processing take place? This must include data backup/archival locations.	
In order to protect against/reduce impact of security or privacy breach, has the supplier taken an insurance policy with an insurance provider?	
Where will your ICT support staff be accessing departmental data from?	
Supplier Supporting Documentation	
Please attach the following documents for review (if existing):	
Relevant SOC Type 2, IRAP or ISO 27001 certification reports dated within 2 years.	Stop here if attached and return reports with questionnaire. Security team will review and contact you if they have any further questions.
Other independent audit reports dated within 3 years.	
Subject	Supplier responses
Does your entity have a set of policies for information security and privacy approved and released by senior management?	
Are they published and communicated to all relevant stakeholders?	
Is your security and privacy policies based on or compliant with an industry based standard (e.g. ISO27002, NIST, etc.)? Please list.	
Does your security policy cover the use of mobile devices?	
Have these policies been reviewed within the last 12 months?	
Do you have security policies covering third-party (e.g. supplier) arrangements?	
Do your contracts cover third-party arrangements and include security requirements they must abide by?	
Do you assess your third parties? How often?	
Risk Management	Supplier responses
Does your organisation have an internal risk management policy based on an industry standard?	
Does the supplier conduct independent reviews/audits of the service/system, in order to provide assurance that the information security policy has been implemented effectively? If so, who conducts such reviews and what is the frequency?	

Does your organisation record the results of information security risk assessments and treatments in its risk register?	
Have your risks been reviewed within the last 12 months?	
Does your organisation maintain a business continuity and disaster recovery plan?	
Is the plan tested on a regular basis? If so, how often?	
Security Responsibilities	Supplier responses
Are all stakeholders general security responsibilities defined and communicated to stakeholders?	
Do you have dedicated security positions with established responsibilities (e.g. CISO, Security manager)? Please list.	
Do you segregate duties to reduce the opportunity for misuse of information?	
Asset Management	Supplier responses
Does your organisation maintain an inventory of assets with identified owners?	
Does your organisation have a documented around the acceptable use of organisation information assets?	
Have these assets been audited within the last 12 months?	
Information classification	Supplier responses
Does your organisation classify data held (e.g. Government information, legal requirements, customer data, sensitivity)?	
What has this data been classified at?	
Has a privacy impact assessment been carried out?	
Is there Agency PII?	
Do you have systems in place to prevent the loss of data based on its classification?	
Is there a data loss prevention (DLP) solution in place for any components storing customer data (i.e. servers, end user devices, Email, FTP, etc.)? Please explain.	
Is Agency's data kept physically and/or logically separated from other supplier's clients data? If so, describe the methods used.	
Does the supplier have data retention and sanitisation policy and procedures? If so, please explain.	
Information Security Media Management	Supplier responses
Does your organisation have procedures in place to detect and respond to the unauthorised removal of media?	
Do you have procedures in place to dispose of media in a secure fashion?	
Access control	Supplier responses
Does your organisation have a formal policy on who accesses sensitive information?	
Do you restrict access via ICT systems to only those specifically authorised to access information? How?	
Do you manage privileged access (i.e. administrative access) to networks and devices in accordance with industry standards? If yes, please list.	
Is your system and information access reviewed at least every 12 months?	
Are supplier staff able to access customer data? If so, 1. Which groups of staff (roles) have access to customer data? 2. Does staff access customer data on a strictly 'need to know' basis? 3. Has access control system(s) been established for system components that restricts access based on a user's 'need to know', and is set to 'deny all' unless specifically allowed?	
Personnel Security	Supplier responses
Employee Screening	
Do you conduct background screening of all members of staff, contractors and other parties involved in the program of work you are applying for?	
Are information security terms and conditions part of employee agreements?	
Are employees and stakeholders required to sign confidentiality agreements to protect customer information?	
Does the supplier have a formal disciplinary process for employees who have violated the security policies and procedures?	
Have all members of staff, contractors and other parties involved in the program of work you are applying for completed dedicated information security training and awareness within the last 12 months?	
Does your organisation train, or have training available, for members who handle information?	

Are members trained/informed to not access sensitive information and limit access to sensitive information to others?	
Do you run Social Engineering training - i.e. Phishing?	
Does your organisation manage Australian recognised security clearances?	
Role Changes	Supplier responses
Does your organisation have documented procedures which govern when changes in role, including termination occur, including the removal or access and return of assets?	
Physical Security	Supplier responses
Does your organisation plan and document physical security measures?	
Does your organisation employ monitored security (e.g. guards, alarms, etc.) on its facilities providing services to government?	
Do physical entry controls prevent visitors, deliveries and contractors entering sensitive areas?	
Do you have increased physical security requirements for areas with sensitive information, including systems (e.g. servers)?	
Do you employ physical systems to prevent fire, flood, power loss impacting on sensitive information, including systems?	
Supplier Security Audit - ICT Security	Supplier responses
Security Documentation and Planning	
Does your organisation have system security plans?	
Has your organisation undertaken an independent ICT security assessment within the last 12 months?	
Do you test the security of systems, developed and purchased, prior to operational use?	
Do you have a cyber security strategy?	
Does your organisation have a dedicated ICT security manager (or equivalent)?	
Incident Response	Supplier responses
Does your organisation maintain a security incident/privacy breach response plan articulating roles and responsibilities?	
Has your incident response plan been tested within the last 12 months? Do you run tabletop exercises at least once a year?	
Has the supplier suffered a data loss or security breach within the last 3 years? If so, please explain.	
Does the supplier notify the Agency when an incident and or breach that may affect the security of their information or interconnected systems is detected or reported? If so what is the timeframe mandated by your policy?	
Will the supplier share RCA (Root Cause Analysis) of detected security incident or breach with the Agency?	
IT Systems and Third Parties	Supplier responses
Who are your cloud service providers who will store Agency information?	
Do third parties have access to your customer data?	
Does your organisation utilise a managed services provider to provide IT services? If so, who?	
If so, are your security requirements detailed in your contract?	
Does the supplier review or audit security posture of their partners/suppliers/sub-contractors? If so, how frequently?	
ICT System Hygiene	Supplier responses
Are you compliant with ASD's essential 8?	
Do you have an internal password policy?	
Do you have complexity or length requirements for passwords?	
Are your administrators required to use MFA?	
Do you log system and network security events for at least 90 days?	
Do your systems run anti-malware and virus protection programs?	
Are all devices that connect directly to your networks centrally managed?	
How do you limit data exfiltration?	
Is the technical configuration of your systems independently audited at least every 12 months?	
Does your organisation have a policy to manage legacy ICT equipment and software?	
Are secure coding practices adopted by the supplier's in-house software development team and/or their providers? If so, please name the methodologies used (e.g. MS SDL, OWASP CLASP, BSIMM, etc.).	

Do you have a formal ICT change policy and process and is it strictly followed?	
Are sufficient security controls deployed for data in transit and at rest? i.e. encryption of data	
Are sufficient security controls deployed for external/public/customer access to the service/system? i.e. MFA	
Are you confident you are aware of all access points to your data externally? i.e. exposed API's and that they have all been penetration tested?	
Do you have backups in place and have they been restore tested?	
Vulnerability Management	Supplier responses
Do you have a vulnerability management process, program or policy?	
Are operating systems regularly patched and at current patch levels?	
Do you path critical vulnerabilities within 48 hours?	
Do you use centrally managed tools to manage vulnerabilities?	
Are vulnerability scans and penetration tests performed on systems (i.e. Infrastructure, OS, Application), in scope of the service?	
1. If so, what is the frequency?	
2. Is it performed by an independent third-party or In-house team?	
3. Please attach the latest vulnerability assessment and penetration test reports.	

Annexure B — Information Transfer Log (Template)

Maintain a record for all confidential or PII information transferred externally (physical or electronic):

- **Date/time of transfer**
- **Transfer method** (courier, secure file transfer, etc.)
- **Media type** (e.g., USB, HDD, encrypted file)
- **Identifying numbers** (media serial/asset IDs)
- **Recipient** (name, organisation, contact)
- **Description of information** (classification; brief summary)
- **Purpose of transfer**
- **Authorising officer**
- **Controls applied** (encryption/password, tamper-evident packaging, two-factor authentication)
- **Confirmation of receipt** (tracking number, signed receipt, delivery log)